PCT/KR 2004/000739
RO/KR 31.05.2004
Rec'd PCT/PTO 28 SEP 2005
10/551344

# 대한민국특허청
# KOREAN INTELLECTUAL PROPERTY OFFICE



별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0036113
Application Number

출 원 년 월 일 : 2003년 06월 04일
Date of Application JUN 04, 2003

출 원 인 : 박미경
Applicant(s) PARK MI KYOUNG

2004 년 05 월 19 일

특 허 청
COMMISSIONER

**PRIORITY DOCUMENT**
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

【서지사항】

| | |
|---|---|
| 【서류명】 | 특허출원서 |
| 【권리구분】 | 특허 |
| 【수신처】 | 특허청장 |
| 【제출일자】 | 2003.06.04 |
| 【발명의 명칭】 | 알에프 태그에 저장된 제품 확인 정보를 판독할 수 있는 이동통신 단말기 및 그 단말기와 통신하는 컴퓨터에서 실행 가능한 서비스 관리 방법 |
| 【발명의 영문명칭】 | Mobile phone capable of reading genuine article verifying information stored in a RF-tag and method for administrating service management executable in a computer communicating with the same phone |
| 【출원인】 | |
| 【명칭】 | 주식회사 텔텍 |
| 【출원인코드】 | 1-1998-613350-0 |
| 【출원인】 | |
| 【성명】 | 박미경 |
| 【출원인코드】 | 4-2003-011882-2 |
| 【대리인】 | |
| 【명칭】 | 특허법인 엘엔케이 |
| 【대리인코드】 | 9-2000-100002-5 |
| 【지정된변리사】 | 변리사 이헌수 |
| 【포괄위임등록번호】 | 2003-020780-9 |
| 【포괄위임등록번호】 | 2003-020326-6 |
| 【발명자】 | |
| 【성명】 | 박미경 |
| 【출원인코드】 | 4-2003-011882-2 |
| 【발명자】 | |
| 【성명의 국문표기】 | 현광철 |
| 【성명의 영문표기】 | HYUN,KWANG CHUL |
| 【주민등록번호】 | 490826-1011818 |
| 【우편번호】 | 137-070 |
| 【주소】 | 서울특별시 서초구 서초동 1608-2, 서건아트빌라 303호 |
| 【국적】 | KR |
| 【심사청구】 | 청구 |

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
특허법인 엘엔케이 (인)

【수수료】

| | | | |
|---|---|---|---|
| 【기본출원료】 | 20 | 면 | 29,000 원 |
| 【가산출원료】 | 54 | 면 | 54,000 원 |
| 【우선권주장료】 | 0 | 건 | 0 원 |
| 【심사청구료】 | 22 | 항 | 813,000 원 |
| 【합계】 | 896,000 원 | | |
| 【감면사유】 | 소기업 (70%감면) | | |
| 【감면후 수수료】 | 268,800 원 | | |

【첨부서류】 1. 소기업임을 증명하는 서류_1통

【요약서】

【요약】

본 발명은 각종 브랜드 상품에 부착되어 해당 제품의 진품 여부를 판정할 수 있도록 하는 비접촉식 통신 태그 및 태그의 정보를 판독할 수 있는 태그판독기 기능을 갖는 이동 통신 단말기에 관한 것이다.

본 발명에 따른 태그판독기 기능을 갖는 이동 통신 단말기는 보유하고 있는 다수의 암호키 중 태그에 저장된 암호키와 대응되는 암호키를 태그로부터 수신한 신호에 기초하여 특정한다. 이동 통신 단말기는 태그로부터 암호화된 제품 정보를 수신하여 이를 이 암호키에 의해 복호화하고 그 결과를 표시부에 평문으로 표현한다. 진품 인증 내역이나 진품 인증 후 구매 완료된 제품에 대한 구매 정보는 이동 통신망을 통해 서비스 관리 서버로 전송되어 마케팅 정보로 활용된다.

또한 본 발명에 따른 비접촉식 통신 태그는 판독기에 의해 제품정보가 판독된 횟수를 비휘발성 메모리에 저장하며, 판독 요청시 판독 횟수가 미리 정해진 기준값 이상이면 제품정보의 추가적인 판독을 차단한다. 이에 의해 정당한 태그가 제품 사용 후에 부정하게 재사용되는 것을 방지한다.

나아가 본 발명의 특징적인 양상에 따라 태그와 이동 통신 단말기간의 통신 과정에대한 재전송 공격을 차단하기 위하여 교환하는 메시지마다 난수를 발생시켜 포함시키고 이를 체크한다. 또 내구재의 경우 비휘발성 메모리에 기록된 데이터가 장기간의 보관 과정에서 소실되는 것을 막기 위해 매 판독시마다 데이터를 리프레쉬시키는 것을 특징으로 한다.

【대표도】

도 2

【색인어】

비접촉식 태그, 알에프 태그, 진품 인증, 표시, 리프레쉬, 카운터, 리더, 판독기, 암호화, 3-DES, 이동통신 단말기

【명세서】

【발명의 명칭】

알에프 태그에 저장된 제품 확인 정보를 판독할 수 있는 이동통신 단말기 및 그 단말기와 통신하는 컴퓨터에서 실행 가능한 서비스 관리 방법{Mobile phone capable of reading genuine article verifying information stored in a RF-tag and method for administrating service management executable in a computer communicating with the same phone}

【도면의 간단한 설명】

도 1은 본 발명에 따른 진품 인증 시스템을 개략적으로 설명하기 위한 도면이다.

도 2는 본 발명에 따른 비접촉식 통신 태그의 구성을 도시한다.

도 3은 본 발명에 따른 이동 통신 단말기의 전체적인 구성을 개략적으로 도시한 블럭도이다.

도 4는 본 발명의 일 실시예에 따른 태그와 이동통신단말기간의 통신 과정을 설명하는 도면이다.

도 5는 본 발명의 바람직한 일 실시예에 따른 판독기간의 인증 과정을 설명하는 도면이다.

도 6a는 본 발명에 따른 암호화/복호화부(210)의 제 3 실시예에 따른 암호키들의 일 예를 도시한다.

도 6b는 본 발명에 따른 암호화/복호화부(210)의 제 8 실시예에 따른 암호키들의 일 예를 도시한다.

<도면의 주요부분에 대한 부호의 설명>

10 : 비접촉식 통신 태그

20 : 이동통신단말기

100 : 비접촉식 통신 수단

110 : 안테나

131 : 전원공급부

133 : 복조부

135 : 변조부

200 : 제어부

210 : 암호화/복호화부

220 : 유출 암호키 갱신부

230 : 재전송 공격 차단부

250 : 정보 제공부

270 : 사후 관리 처리부

290 : 리프레쉬

300 : 저장부

500 : 태그통신부

510 : 안테나

531 : 전력 송출부

533 : 복조부

535 : 변조부

700 : 제어부

710 : 암호화/복호화부

720 : 리프레쉬 처리부

730 : 재전송 공격 차단부

750 : 정보판독부

760 : 정보 전송부

770 : 판독기 인증부

790 : 유출 암호키 갱신부

910 : 저장부

930 : 조작부

950 : 표시부

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<25> 본 발명은 이동 통신 단말기에 관련되며, 특히 각종 브랜드 제품에 부착되어 해당 제품의 정보를 제공하는 알에프 태그 및 그 태그의 정보를 읽어 표시함에 의해 진품 여부를 판정할 수 있도록 하는 태그 판독 기능을 가진 이동 통신 단말기에 관한 것이다.

<26> 일본 공개특허공보 평14-215749호나 평14-209692호에 개시되어 있는 바와 같이 제품 정보가 전자적으로 기록되고 비접촉방식의 통신을 하는 태그(이하 "태그"라 한다)와 이 정보를 판독하는 휴대형의 태그판독기를 이용하여 제품 정보를 확인하고 구매나 물품 관리에 도움을 주고자 하는 기술이 알려져 있다. 그러나 이 기술은 제품의 진위 여부를 확인하고자 하는 목적을 갖고 있지 않고 따라서 정보의 기록이나 판독 과정이 매우 취약하여 정보의 위조나 정보 판독의 조작이 가능하다.

<27> 또다른 종래기술에 국내 공개특허공보 제2002-0085144호, 일본 공개특허공보 평13-354310호, 일본 공개특허공보 평13-341810호 등에는 비접촉식 통신 태그에 전자적으로 기록된 제품정보를 판독하고 인터넷과 같은 통신 네트워크를 통해 제품관리 데이터베이스에 조회하여 해당 제품의 진위 여부를 판단하는"네트워크형" 진품 확인 시스템이 개시되어 있다.

<28> 그러나 이 같은 네트워크형 시스템을 이용하기 위해서는 유선인 경우에는 판독 장치를 데스크톱 형태로 제작할 수 밖에 없고 따라서 진품 확인을 위해서는 특정한 장소를 방문해야만 하는 불편함이 있다. 또한 무선인 경우에도 싸이즈가 커짐에 따라 휴대가 어렵고 원가가 비쌀 뿐 아니라 이용시에는 무선 통신망 이용료를 부담해야 하는 추가적인 문제점이 있다. 더구나

데스크톱 형태라면 특정한 장소에서만 조회가 가능하므로 물품을 구입하기 전에 미리 확인하기 어려운 문제점이 있다. 나아가 이 같은 방식의 경우 동일한 진품 인증 코드를 복사하여 사용하는 모조품의 경우에는 대응이 어려운 문제점이 있다.

<29> 또다른 종래기술에 일본 공개특허공보 평12-348148호, 일본 공개특허공보 평12-148950호에는 태그판독기가 비접촉식 통신 태그에 전자적으로 기록된 제품정보를 판독하고, 이 판독된 정보를 자체적으로 미리 저장되어 있는 기준 데이터(제품번호, 제조일자, 제품 생산 브랜드명, 관리 이력 정보, 제품 설명등)와 비교하여 제품의 진위여부를 판단하는 기술이 개시되어 있다.

<30> 그러나 이 같은 오프라인 방식의 인증 장치는 위에 기술한 네트워크형 시스템의 문제점은 해결하고 있지만 태그판독기에 각 제품별 제품정보를 미리 모두 저장하고 있어야 하므로 메모리 용량이 커질 뿐 아니라 판독기가 진품 여부를 자체 판단해서 그 결과만을 제시하므로 사용자가 인증 과정의 정보를 직접 확인하지 못하여 신뢰성을 확신하지 못하는 문제점이 있다. 즉, 이 장치는 제품 판매자의 입장만을 고려하고 있으며 제품 구매자의 요구를 충분히 만족시키지 못하고 있다. 나아가 이 장치의 경우 판독기를 구입한 이후에 출시되는 신제품 혹은 추가로 가입된 회사의 제품들에 대해서는 진품 확인이 불가능하거나 또는 기 출하된 모든 판독기에 대해 제품 정보를 갱신해 주어야 한다는 치명적인 문제점을 안고 있다.

<31> 또 이들 선행기술들은 태그 자체를 제품에서 떼어내어 모조품에 부착할 경우에는 아무런 대책이 없다.

<32> 이러한 태그의 재사용 문제점을 해결하고 있는 또다른 종래기술에 국내 공개특허공보 제2001-0089216호, 국내 등록실용신안공보 제252202호, 일본 공개특허공보 평 제12-251164호가 있다. 이 기술은 제품 정보가 저장되고 해당 제품에 부착된 비접촉식 통신 태그와 태그판독기

를 포함하여 구성되는 진품 확인 장치로, 태그를 제품에서 떼어내면 안테나와 같은 부분이 파괴되도록 하여 태그 자체를 재활용하지 못하도록 하는 방식이다. 그러나, 이러한 기술은 적용 대상이 병입 제품 등 특수한 제품에만 한정되고 태그의 물리적인 파괴를 막도록 사전 조치가 가능할 수도 있다는 문제점이 있다. 또한 태그 자체가 파괴됨에 따라 사후에 제조사 조차도 태그 판독 이력 정보를 읽어내어 고객 지향 마케팅 등에 활용하는 것이 불가능하다는 문제점을 여전히 가지고 있다.

【발명이 이루고자 하는 기술적 과제】

<33> 본 발명은 이러한 문제점을 해결하고자 하는 것으로, 구매자 입장에서 간편하면서도 진품을 구매한다는 신뢰감을 극대화할 수 있는 진품 확인 장치를 제공하는 것을 목적으로 한다.

<34> 나아가 본 발명은 네트워크에 접속이 필요하거나 판독기를 업그레이드하지 않고도, 판독기의 구입 이후에 추가되는 신제품에 대해서도 진품 여부의 확인이 가능한 진품 확인 장치를 제공하는 것을 또다른 목적으로 한다.

<35> 또한 본 발명은 하나의 태그판독기로 의류, 신발류, 가죽제품류, 주류, 농수축산품, 의약품, 전자제품, 기계류제품 등 구매시에 진품 확인이 필요한 제품 뿐 아니라 귀금속류, 예술품과 같이 지속적이고도 장기적으로 진품 확인이 요구되는 제품까지, 더 나아가 감정서, 입장권, 각종 증명서 및 시설이용권, 금권, 유가증권, 중요서류 등 광범위한 종류의 물품들에 대해 일반적으로 적용할 수 있는 진품 확인 장치를 제공하는 것을 또다른 목적으로 한다.

<36> 추가적으로, 본 발명은 태그를 물리적으로 파괴하지 않고도 모조품에 진품 태그가 재사용 혹은 도용되는 것을 차단하는 것이 가능한 진품 확인 장치를 제공하는 것을 또다른 목적으로 한다.

<37> 나아가 본 발명은 이동 통신 단말기와 일체로 제작되어 누구나 편리하게 소지할 수 있는 태그판독기를 소비자에게 제공함으로써, 판매자 입장에서는 임의의 구매자가 판독기를 소지하고 있을지 모르므로 모조품을 제시하기 어려워지고 구매자 입장에서는 언제 어디서든지 진품 여부를 편리하게 확인할 수 있도록 하는 것을 또 다른 목적으로 한다.

<38> 상기 목적을 달성하기 위한 본 발명의 일 양상에 따른 진품 확인 장치는 제품에 부착된 비접촉식 통신 태그와, 이 태그에 전자적으로 기록된 제품 정보를 판독하는 이동 통신 단말기에 구현된 태그판독기로 구성된다.

<39> 본 발명의 특징적인 양상에 따라 태그에는 디지탈 형태의 제품 정보가 전자적으로 저장된다. 여기서 제품 정보는 텍스트 파일과 같은 평문 형태로 저장되거나, 또는 이후에 이동통신단말기에 저장된 테이블로부터 해석되어질 수 있는 하나 이상의 코드로 인코딩되어 저장될 수 있다. 태그는 이동통신단말기로부터의 요구에 따라 저장된 제품 정보를 추출하고 이를 암호화하여 무선 신호로 출력한다.

<40> 이동통신단말기에는 태그가 출력하는 암호화된 제품 정보를 해독할 수 있는 암호키와, 읽어들인 제품 정보를 가시적인 정보로 표시하는 표시부가 구비된다. 정당한 태그가 부착된 제품인 경우에는 적절한 제품 정보가 표시되지만, 그렇지 않은 제품인 경우에는 읽을 수 없는 정보가 표시되거나 모조품 경고 메시지가 표시된다.

<41> 즉, 본 발명에 따른 진위 인증 장치는 별도의 인증정보를 서버로 조회하거나 복잡한 인증코드를 사용하지 않고, 대신에 태그에 저장된 제품 정보를 읽어 일반인이 이해할 수 있는 형태로 표시부에 표시하되, 배포가 제한된 암호키를 이용하여 모조 태그의 사용을 차단한다. 다시 말하면, 종래의 진위 확인 장치들은 특수한 인증코드 등의 검증을 이용하는데 반해 본 발명은 암호화/복호화 자체를 진위 검증 기술로 채택한다.

<42> 이에 따라 본 발명에 따른 진위 인증 기술은 암호 기술에 의해 모조 태그를 차단하면서도, 동시에 휴대용 단말기의 화면에 제품 정보를 표시하여 구매자가 직접 눈으로 확인할 수 있으므로 신뢰감을 극대화할 수 있다.

<43> 나아가 본 발명에 따른 진위 인증 장치는 표시부에 문장으로 표현되는 제품정보에 의해 제품 식별이 가능하므로 상이한 제품에대해 동일한 암호키를 사용하는 것이 가능하고, 따라서 판독기에 저장된 암호키의 수에 구애받지 않고 많은 제품에 적용할 수 있는 장점을 가진다. 더 나아가 판독기가 판매된 이후에 추가된 제품에 대해서도 동일한 암호키를 적용하여 진위 인증을 해줄 수 있는 극적으로 유리한 효과를 가진다. 따라서 이동통신단말기에 한정된 수의 암호키를 저장하고 있는 상태에서조차도, 새로운 상품을 정품 인증 대상에 추가하여 그 상품의 제품 정보를 판독하는 것이 가능하다.

<44> 모든 제품에 대해 단일의 암호키를 적용하는 것도 가능하지만, 이 경우 키가 유출되면 피해가 커진다는 문제점이 있다. 이에 대비하는 본 발명의 또다른 양상에 따르면, 태그에는 업종, 제조업체, 브랜드, 제품명 등의 기준에 따라 정해지는 하나의 암호키가 저장되지만, 이동통신단말기에는 모든 종류의 태그를 읽을 수 있도록 복수의 암호키들이 저장된다. 이에 따라 일부 업종, 제조업체, 브랜드 또는 제품의 암호키가 유출된 경우에도 나머지들에 대해서는 보안이 유지될 수 있다. 나아가 여유분의 암호키를 확보하여 이동통신단말기에 미리 저장해둔다면, 일부 암호키가 유출된 경우에도 새로운 암호키를 할당하고 판독기를 업그레이드함으로써 추가로 출고되는 제품에 대해서는 모조 태그의 사용을 막을 수 있다.

<45> 본 발명의 또다른 양상에 따르면, 태그에는 업종, 제조업체, 브랜드, 제품명 중의 적어도 2개의 기준에 따라 구분되어 할당된 적어도 2 개의 암호키들이 저장되고, 제품 정보는 이들 복수의 암호키들이 순차적으로 사용되어 암호화된다. 이에따라 암호키들 중 일부가 유출된다

하더라도 해당 업종, 해당 제조업체, 해당 브랜드 또는 해당 제품 등 해당 범위로 위험이 제한되는 장점이 있다.

<46> 본 발명의 특징적인 또다른 양상에 따르면, 이동통신단말기는 자체에 저장되는 하나 혹은 그 이상의 씨드(seed) 값을 이용하여 수많은 암호키를 생성할 수 있는 알고리즘을 내장하며, 태그에는 이에 필요한 하나의 암호키와 이를 생성하는데 필요한 암호키 생성 정보가 저장된다.

<47> 이에 따라 본 발명에 따른 이동통신단말기는 한정된 메모리로도 수많은 암호키를 확보하는 것이 가능하여, 이미 판독기를 취득한 이후에도 수많은 업체, 브랜드 또는 제품에 대해 새로운 암호키를 부여하여 진품 인증 대상에 추가하는 것이 가능하다.

<48> 나아가 일부 업체, 브랜드 또는 제품의 암호키가 유출된 경우에도 나머지 업체, 브랜드 또는 제품에 대해서는 암호키가 달라 보안이 유지될 수 있고, 암호키가 유출된 경우에는 새로운 암호키를 할당하고 판독기를 업그레이드함으로써 추가로 출고되는 제품에 대해서는 모조 판독기 및 모조태그의 사용을 막을 수 있는 여지를 더욱 충분히 확보할 수 있게 된다.

<49> 본 발명의 또다른 특징적인 양상에 따라 본 발명에 따른 정품 인증 장치는 암호키가 유출된 경우에 피해를 최소화할 수 있는 방안이 강구된다. 특정한 물품에 부착된 태그에 저장된 하나 혹은 다수의 암호키가 유출된 경우 제조사는 새로 제조하는 태그에 기존과는 상이한 암호키를 할당하여 저장한다. 이 암호키는 기존에 배포된 태그판독기기에 이미 저장되어 있는 다수의 암호키 중 하나이다. 본 발명의 특징적인 양상에 따라 이 태그에는 판독기로 하여금 유출된 암호키에 대해 기존에 할당된 암호키를 폐기하고 새로 할당된 암호키로 대체하도록 처리하는 제어로직이 추가된다. 암호키가 유출된 후 새로 제작된 태그가 부착된 제품에 대해 판독기가 제품 정보를 읽으면, 판독기 혹은 이동통신단말기의 암호키 할당 정보가 자동으로 업그

레이드된다. 이후에는 업그레이드된 판독기는 기존의 암호키에서 동작하는 모조 태그가 부착된 제품은 모조품으로 판정하는 것이 가능하다.

<50> 본 발명의 또다른 양상에 따르면, 태그에는 판독기 혹은 이동통신단말기에 의해 판독된 횟수가 저장되며, 일정 횟수 이상 판독되면 추가적인 판독을 차단한다. 본 발명의 이 같은 양상에 따라 태그를 물리적으로 파괴하지 않고도 정품 태그가 모조품에 부착되어 재사용되는 것을 차단할 수 있다. 보조적인 양상에 따르면, 지정 판독 가능 횟수 이상으로 판독된 경우에도 공장의 특수한 암호 키를 가진 판독기에 의해 제품 정보는 물론 판독 시마다 저장된 이력 정보가 판독될 수 있다.

<51> 본 발명의 또 다른 양상에 따르면, 태그와 판독기 혹은 이동통신단말기의 통신에는 암호화에 추가하여 난수에 기초한 재전송 공격 차단 알고리즘이 적용된다. 재전송 공격 차단 알고리즘은 통신 과정에서 암호화된 문장 자체를 해킹하여 재 전송함으로써 로그인 등 필요한 인증 처리를 얻어내는 것을 차단하기 위한 기술이다. 이에 따르면 매 정보 교환 세션마다 난수를 발생하여 평문과 함께 암호화하여 보내고 그 응답으로 수신되는 정보에서 난수를 추출하여 동일성을 체크함에 의해 불법적인 재전송 공격을 차단한다. 본 발명은 이 같은 기술을 채택하므로 통신 과정을 도청하여 신호 패턴을 저장한 후 재전송 공격하거나 불법적인 태그를 복제하고자 하는 시도가 차단되어 정품 인증의 신뢰성을 더욱 높일 수 있다.

<52> 본 발명의 추가적인 양상에 따르면, 태그판독기는 이동 통신 단말기에 일체화되어 구현된다. 이동통신단말기는 판독 내역 정보를 이동 통신망을 통해 진품 인증 서비스 관리 서버로 전송한다. 서비스 관리 서버는 수신한 판독 내역 정보를 사용자별로 취합하여 고객관리 정보로 제공한다. 이때 이동통신 단말기의 식별정보를 이용하여 가입자 서버로부터 해당 단말기

소지자의 신상을 자세히 알 수 있으므로 취합된 데이터를 효과적으로 분류하고 처리할 수 있다.

<53> 본 발명의 또다른 추가적인 양상에 따라 이 판독 내역 정보는 구매 정보를 포함한다. 사용자가 특정한 제품에 대해 진품 인증한 후에 구매 완료 키를 누르게 되면 해당 물건을 구매했다는 구매 정보가 서비스 관리 서버로 전송되거나 또는 이동 통신 단말기 자체의 메모리에 취합된 후 이후에 일괄 전송된다. 서비스 관리 서버는 수신한 판독 내역 정보를 사용자별로 취합하여 고객관리 정보로 제공한다.

<54> 누구나 소지하는 이동 통신 단말기와 일체로 태그판독기가 제공됨에 따라 구매자가 이동통신단말기를 휴대하면서 언제 어디서나 다양한 종류의 제품에 대해 진품 여부를 확인하는 것이 가능하므로 판매자는 어느 구매자가 진품 확인을 할지 몰라 모조품 판매의 유혹을 차단 당하게 된다.

<55> 또 다른 본 발명의 양상에 따르면, 본 발명에 따른 태그는 저장장치로 비휘발성 메모리를 사용하고, 판독 동작 때마다 메모리를 리프레시 시킴에 의해 통상 10년을 넘기기 어려운 정보 저장 기간을 연장함으로써 예를 들면 골동품, 예술품, 감정서, 고급의류 등 내구재에도 적용할 수 있도록 한다.

<56> 또한 본 발명의 특징적인 양상에 따른 태그는 메모리에 저장된 프로그램에 의해 제어되는 마이크로프로세서가 아닌 디지털 로직으로 설계된 전용 하드웨어에 의해 제어된다. 이에 따라 통상 저장된지 10년이면 프로그램이 소실되어 동작할 수 없는 문제점을 해결하여 영구적으로 제어부가 동작하는 것이 가능하다.

<57> 본 발명의 추가적인 양상에 따르면, 이동통신단말기간에도 상호간에 인증을 수행함으로써 상호간에 태그판독기 자체의 신뢰성을 확인할 수 있도록 한다. 이에 따라 모조 비접촉식 통신 태그를 대상으로 동작하는 모조 휴대형 판독기가 사용되는 것도 방지할 수 있다.

【발명의 구성 및 작용】

<58> 본 발명의 이와 같은, 또 다른 추가적인 양상은 첨부된 도면을 참조하여 후술하는 바람직한 실시예들을 통하여 더욱 명백해질 것이다. 이하에서는 본 발명을 이러한 실시 예를 통해 당업자가 용이하게 이해하고 재현할 수 있도록 상세히 설명하기로 한다.

<59> 도 1은 본 발명의 동작을 개략적으로 설명하기 위한 도면이다. 도시된 바와 같이 본 발명은 의류, 신발류, 가죽제품류, 주류, 농수축산품, 의약품, 전자제품, 기계류제품, 귀금속류, 예술품, 감정서, 입장권, 각종 증명서 및 시설이용권, 금권, 유가증권, 중요서류 등 각종 제품에 부착된 비접촉식 통신 태그(10-1, 10-2, 10-3)와, 이 태그의 정보를 읽어 표시하는 이동통신단말기(20-1, 20-2)로 구성된다.

<60> 바람직한 일 실시 예에 있어서, 비접촉식 통신 태그는 가로 세로가 각각 10-18㎜ 정도인 사각형이며 박형인 수동 태그이다. 태그판독기(20-1,2)는 본 발명의 특징적인 양상에 따라 이동 통신 단말기와 일체로 제공되어 개인이 휴대하기에 편리하고, 배터리에 의해 구동되며 전면에 표시부를 가지고 있다.

<61> 판독기를 가진 개인은 위에서 언급한 비접촉식 통신태그가 부착된 어떠한 종류의 제품이든 자신의 이동통신단말기를 제품에 근접시킴으로써 제품의 정보를 표시부에서 확인할 수 있을 뿐 아니라 동시에 브랜드의 진위 여부를 판별하거나 모조 제품을 구별할 수 있게 된다.

<62> 본 발명에 따른 태그판독기는 이동 통신 단말기와 일체로 제공되므로 판독기에 의해 판독된 정보판독 내역을 이동 통신망을 통해 진품 인증 서비스 관리 서버(40)로 전송하는 것이 가능하다. 본 발명의 특징적인 양상에 따라 정보 판독 내역은 판독 대상 제품마다 고유하게 할당된 제품 고유번호 및 이동 통신 단말기마다 고유하게 할당된 판독기 고유번호를 포함한다. 바람직한 일 실시예에 있어서, 정보 판독 내역은 업종, 제조업체, 브랜드, 제품명, 등급, 모델명, 생산지, 제조일, 일련번호, 가격, 인증 일시 등의 진품 인증 내역 정보를 추가로 포함한다. 또다른 실시예에 있어서 정보 판독 내역은 진품 인증된 제품 중 구매 완료된 제품에 대한 구매 정보를 포함한다. 구매 정보는 상기 진품 인증 내역 정보에 부가하여 구매가격, 구매 일시 등의 정보를 포함할 수 있다.

<63> 진품 인증 서비스 관리 서버(40)는 이동 통신 단말기로부터 정보 판독 내역 정보를 수신하면(단계 ①②), 수신한 내역 정보에 포함된 이동 통신 단말기의 식별정보로부터 이동통신사의 가입자 서버(30)로 조회하여 해당 가입자의 신상 정보를 획득하는 것(단계 ③)이 가능하고 이에의해 더욱 세분화된 고객 관리가 가능하다.

<64> 즉, 가입자 서버(30)에는 이동 통신 회사에 의해 가입자의 성별, 연령, 주소, 학력, 직업, 취미 등 상세한 신상 정보가 저장되어 있다. 서비스 관리 서버(40)는 수신한 정보 판독 내역 정보와 이 같은 가입자 정보를 취합하여, 예를 들면 특정한 연령대의 사람들의 구매 성향이나, 또다른 예에 있어서 특정한 직업을 가진 사람들의 구매 성향, 제품 선호도 등을 조사하는 것이 가능하다. 이 같은 정보는 진품 인증 대상 제품을 생산하는 생산자에게는 매우 유용한 마케팅 정보가 될 수 있다. 서비스 관리 서버(40)는 이 같이 취합된 정보들을 고객관리 정보로 저장하며, 이후에 서비스 대상 제품들을 제조하는 제조사들이나 또는 인증 서비스 관리 회사의 요구에 응답하여 보고서를 작성하여 출력한다. 또는 이 같은 보고서를 수시로 작성하

여 네트워크로 통신 가능한 브랜드 보유사의 서버(50)로 전송한다(단계 ④) 이 같은 마케팅 보고서의 작성 기술은 당해 분야에서 공지된 것이므로 상세한 설명은 생략한다.

<65> 한편, 이 같은 정보 취합은 구매 완료시나 또는 진품 인증이 어느 정도 수행된 후 정기적으로 또는 비정기적으로 사용자의 조작에 의해 수동으로 진행될 수 있다. 또다른 실시예에 있어서, 단말기에 특정한 응용프로그램을 탑재함에 의해 이 같은 정보의 업로드(upload) 과정이 사용자에게는 묵시적으로 행해질 수 있다. 이 응용프로그램은 정보 축적량과 통신 상태를 감시하다가 음성 통신 또는 데이터 통신 중에 특정한 데이터 채널을 할당받아 축적된 판독 내역 정보를 전송한다. 또다른 실시예에 있어서, 특정한 응용 프로그램은 정보 축적량을 감시하다가 일정한 량에 도달하면 축적된 정보를 단문 메시지 형태로 서비스 서버로 전송한다.

<66> 본 발명의 추가적인 유리한 양상에 따라 서비스 관리 서버(40)는 고객관리 정보로 포인트 정보를 더 포함한다. 즉, 서비스 관리 회사는 구매 정보의 취합에 협조하는 가입자에게 인센티브로 포인트를 적립해주고, 이들 포인트가 적립됨에 따라 상품을 제공하거나 또는 적립된 포인트를 전자 화폐화하여 제휴 싸이트에서 물품 구매에 활용하거나 콘텐츠를 이용하도록 할 수도 있다.

<67> 이 같은 포인트의 적립 처리는 서비스 관리 서버(40)가 판독 내역 정보를 수신하면 수신한 내역 정보의 종류와 내용에 따라 해당 가입자에게 적립 처리하여 이루어진다. 예를 들어 구매 완료된 제품의 가격에 따라 차등하여 포인트가 적립될 수도 있고, 제조사나 제품명에 따라 상이한 포인트가 적립되도록 처리할 수도 있다.

<68> 본 발명의 특징적인 양상에 따라 제품 정보 판독 내역 정보를 수신한 이후에 판독 내역 정보에 포함된 제품 정보 고유번호 및 판독기 고유번호가 이전에 수신한 제품 정보 판독 내역 정보와 동일한지를 체크하여 재전송된 내역 정보인지를 추가로 체크할 수 있다.

<69> 즉, 고객이 구매내역 정보를 반복 전송하여 포인트를 축적하고자 하는 시도를 차단하기 위해 서비스 관리 서버(40)는 전문 형식으로 전송되는 구매 내역 정보를 인증한다. 바람직한 일 실시예에 있어서, 이동 통신 단말기는 구매 내역 정보를 전송할 때 판독기의 고유번호와, 판독한 태그의 고유번호를 함께 전송한다. 서비스 관리 서버(40)는 판독기의 고유번호와 태그 고유번호가 동일한 구매 내역 정보를 무시함으로써 동일한 구매 내역 정보가 반복하여 포인트에 반영되는 것을 차단한다.

<70> 도 2는 본 발명의 바람직한 일 실시 예에 따른 비접촉식 통신 태그의 구성을 도시한다.

<71> 도시된 바와 같이, 본 발명의 바람직한 일 실시 예에 따른 비접촉식 통신 태그(10)는 휴대용 태그판독기와 무선으로 데이터를 교환하며, 그로부터 무선으로 수신한 신호 중 전력 성분을 추출하여 이를 전체 시스템의 전원으로 공급하는 비접촉식 통신 수단(100)과, 제품정보와 암호키 정보를 저장하는 저장부(300)와, 저장부(300)에 저장된 제품정보를 암호키로 암호화하여 비접촉식 통신수단(100)을 통해 외부로 출력하는 제어부(200)를 포함한다.

<72> 바람직한 일 실시 예에서 비접촉식 통신 수단(100)은 안테나(110)와, 상기 안테나(110)를 통해 수신되는 신호 중 전력용 전파 신호를 처리하여 전원을 공급하는 전원 공급부(131)와, 수신되는 신호를 복조하는 복조부(133) 및 송신하는 신호를 변조하는 변조부(135)를 포함한다. 안테나(110)는 인쇄된 패턴 또는 코일로 대략 태그의 외주연을 따라 형성되며, 변조부(135), 복조부(133)의 구성은 당해 분야에서 널리 알려진 것이므로 상세한 설명은 생략한다. 본 발명에 따른 태그(10)는 소형이고 박형으로 제작되어야 하므로 수동형(passive type)으로 제작되어야 하며, 따라서 전원공급부(131)는 수신되는 무선 신호에서 전력 성분을 추출하고 이를 전체 시스템의 전원으로 공급한다. 전원공급부(131)의 동작 및 구성은 공지된 것이므로 상세한 설명은 생략한다.

<73> 저장부(300)는 예를 들면 EEPROM, 플래시 롬과 같은 비휘발성 반도체 메모리로 구성되어 전원이 소실된 상태에서도 데이터가 보존된다. 저장부(300)는 물리적으로 읽기 전용과 쓰기/읽기용의 2 개의 메모리로 구성될 수도 있지만, 바람직한 실시 예에 있어서는 쓰기/읽기가 가능한 단일의 비휘발성 메모리로 구성된다.

<74> 바람직한 일 실시 예에 있어서 저장부(300)에 저장되는 데이터에는 태그가 부착되는 제품정보(370), 예를 들면 업종, 제조업체, 브랜드, 제품명, 등급, 모델명, 생산지, 제조일, 출고일, 일련번호 등과 같은 정보가 저장된다. 또한 저장부(300)에는 태그(10)와 이동통신단말기(20)간의 통신을 암호화하는데 필요한 암호키(330)가 저장된다. 또한 저장부(300)에는 이동통신단말기 측에서 암호키를 특정하는데 필요한 암호키 특정정보(310)가 저장될 수 있다. 본 발명의 특징적인 한 양상에 따라 저장부(300)에는 이동통신단말기에 의해 태그의 제품정보가 판독된 횟수를 저장하는 카운터 영역이 있으며, 판독한 판독기나 판독일시와 같은 판독내역정보를 저장한다.

<75> 본 발명에 따른 통신 태그의 바람직한 일 실시 예에 있어서 시스템 전체를 제어하는 제어부(200)는 스테이트 머신(state machine)으로 설계된 디지탈 로직의 전용 하드웨어, 예를 들면 플립플롭과 게이트 기반으로 설계된 ASIC 회로로 구현된다. 이 같은 회로는 상용화된 다양한 CAD 툴의 지원을 받는 당업자라면 용이하게 구현할 수 있는 것이므로 상세한 설명은 생략한다. 이에 의해 본 발명은 별도의 저장된 형태의 메인 프로그램을 이용하지 않아 비휘발성 메모리 상에서 기억의 보존연한에 따른 문제를 회피할 수 있다. 그러나 이 경우에도 태그마다 달라질 수 있는 정보인 제품 정보나 암호키 관련 정보는 비휘발성 메모리에 데이터로 저장된다. 이에 대해서는 본 발명의 특징적인 양상에 따라 후술하는 별도의 대책이 마련된다.

<76> 그러나 본 발명은 이에 한정되지 않으며 또다른 실시예에 있어서 제어부(200)는 마이크로프로세서로 구현되고, 본 발명의 특징적인 기능들을 소프트웨어에 의한 제어로 달성할 수도 있다. 이때 저장부(300)에는 메인 프로그램이 추가로 저장될 수 있다. 또다른 실시 예에서는 저장부(300)는 물리적으로 2 개의 메모리로 구성되어 메인 프로그램을 포함한 일부분은 별도의 메모리에 저장될 수도 있다.

<77> 본 발명의 특징적인 양상에 따라 제어부(200)는 비접촉식 통신수단을 통해 수신한 신호를 복호화하는 한편 송신할 신호를 암호화하여 상기 비접촉식 통신수단으로 출력하는 암호화/복호화부(210)와, 상기 저장부에 저장된 제품정보를 읽어들여 이를 상기 암호화/복호화부로 공급하는 정보제공부(250)를 포함하며, 추가로 재전송 공격 차단부(230), 사후관리 처리부(270)를 포함할 수 있다.

<78> 정보제공부(250)는 이동통신단말기(20)로부터의 명령에 따라 저장부(300)에 저장된 제품정보를 읽어 비접촉식 통신수단(100)을 통해 출력한다. 본 발명의 특징적인 양상 중의 하나에 따라, 정보제공부(250)는 매 판독시마다 저장부(300)의 카운터 값을 증가시키며, 제품정보를 읽기전에 저장된 카운터 값을 확인하여 카운터 값이 소정 값 이상일 경우에는 이동통신단말기(20)의 판독명령에 응답하지 않거나 제품 정보 대신에 판독횟수가 초과된 부적절한 태그임을 알리는 메시지를 출력한다. 그러나 이 경우에도 내부적으로는 카운터 값은 계속 증가되어 기록된다. 이 데이터는 이후 마케팅팀의 특정 단말기로 확인될 수 있다.

<79> 이 같은 처리를 통해 동일한 태그를 진품에서 떼어내어 모조품에 부착하거나 또는 소비된 진품에서 폐 태그를 분리하여 모조품에 부착하여 재사용하는 것을 효과적으로 차단할 수 있다. 종래 기술에서는 강력한 접착제 등으로 태그를 제품에 부착하여 태그를 분리시킬 경우 패턴 인쇄된 안테나가 파괴되도록 하는 등의 물리적인 차단 방식을 채택하였으나 이는 태그 정보

의 사후관리 또는 이용을 위한 접근을 불가능하게 만든다. 뿐만 아니라 이러한 종래 기술은 주의 깊게 태그를 분리시키려고 하는 시도에 대해서는 오히려 불리한 대응일 수 있고 또한 실제 양산 공정에서 이의 구현에도 어려운 점이 있다. 본 발명은 외부에서 접근 불가능한 영역에 카운터 값을 저장하고 이를 체크 함에 의해 물리적인 대책에 비해 비용이 전혀 추가되지 않으면서도 효과적으로 재사용을 차단할 수 있다.

<80> 한편, 예를 들면 상품이 진열대에 진열된 상태에서 이동통신단말기에 의해 수회 판독됨에 따라 이후에 정작 진위 판별이 필요할 때에는 판독이 불가능해지는 경우가 생길 수 있다. 이 같은 문제점을 해결하기 위해 출고시에 태그 노출면에 판독을 차단하는 차폐막을 두는 것이 바람직하다. 차폐막은 예를 들면 알루미늄 박판으로 태그 외면을 감싸서 무선 통신을 차단하는 형태일 수 있다. 이 차폐막은 진위 판별이 필요할 때 태그로부터 분리된다.

<81> 카운터의 판독 제한 기준 값은 제품마다 조정될 수 있다. 예를 들어 양주, 농수축산물과 같은 식품류의 경우에는 출고시 1회, 사용시 2~4회 정도의 사용을 예정하여 카운터 기준값을 3~5 회 정도로 제한하는 것이 좋다. 의류의 경우에는 판매시 및 구입 후에 여러 번의 진품 인증이 있을 수 있으므로 수십회 정도로 하는 것이 좋다. 이 같은 값은 제품 성격이나 유통경로의 단계 수에 따라 적절히 정해질 수 있다.

<82> 그러나 본 발명은 카운터를 체크하여 판독을 제한하는 실시예에 한정되지 않으며, 예를 들면 명화나 골동품, 서류 종류와 같이 판독 횟수의 제한이 없는 경우에도 적용될 수 있는 많은 다른 양상들을 포함하고 있다. 이 경우에 있어서 정보제공부(250)는 정보제공부(250)는 이동통신단말기(20)로부터의 명령에 따라 저장부(300)에 저장된 제품정보를 읽어 비접촉식 통신수단(100)을 통해 출력하며, 매 판독시마다 저장부(300)의 카운터 값을 증가시키지만 카운터 값에 따라 정보 제공을 제한하지는 않는다.

<83> 암호화/복호화부(210)는 비접촉식 통신수단(100)을 통해 송신하는 정보를 암호화하고 그로부터 수신하는 정보를 복호화한다. 바람직한 일 실시예에 있어서 암호화 알고리즘은 3-DES를 사용하지만 이에 한정되는 것은 아니다. 3-DES 알고리즘은 DES 방식을 삼중으로 적용하는 것으로 여러가지 형태가 있으며, 본 실시예에서는 3개의 키를 순차적으로 사용하는 순차연결형(cascaded) 방식의 3-DES를 적용한다. 이들 방식은 모두 대칭키 방식이므로 암호화와 복호화에 동일한 암호키를 사용한다.

<84> 공지된 기술에 있어서 진품 여부의 인증은 태그에 고유한 인증코드를 저장하고 이동통신단말기에서 그 값을 읽어 진품에 해당하는 코드인가를 판단하고 있다. 이에 대해 본 발명은 진품 여부의 인증을 표시부에 표시된 정보를 확인하는 사람의 판단과, 그리고 제품 정보가 올바르게 표시되기 위해 통과해야하는 암호화/복호화과정에 의존한다.

<85> 본 발명에 따른 암호화/복호화부(210)의 가능한 가장 간단한 일 실시예에 있어서, 태그의 저장부(300)에는 단지 하나의 암호키로서 마스터 키(330) 만이 저장되며, 이 마스터 키는 모든 종류의 제품에 있어서 공통적인 유일한 키이다. 이해를 돕기 위해 부연하자면, 이 실시예에 대응되는 이동통신단말기는 이 유일한 하나의 키만 보유하고 있지만, 모든 종류의 제품에 대해 제품 정보의 판독이 가능하다. 암호화/복호화부(210)는 정보 제공부(250)가 외부로 전송하는 정보를 이 암호키로 암호화하며, 외부로부터 수신하여 입력되는 암호화된 메시지를 해독하여 정보 제공부(250)로 제공한다.

<86> 본 발명의 가장 간단한 위 실시예에 있어서도 표시되는 제품 정보에 의해 제품들이 식별될 수 있으므로 수많은 상품에대해 진위 판단을 제공하는 것이 가능하다. 나아가 새로운 제품에 대해 적용될 수 있는 태그가 새로 편입된 경우에 기존의 이동통신단말기를 업그레이드하지 않아도 이 태그의 정보를 읽는 것이 가능하다.

<87> 본 발명에 따른 암호화/복호화부(210)의 제 2 실시예에 있어서, 태그의 저장부(300)에는 단지 하나의 암호키로서 마스터 키(330)와, 이 마스터 키에 대한 암호키 특정정보(310)가 저장된다. 태그를 사용하는 회사들은 다수의 암호키를 준비하고, 예를 들면 업종별 및/또는 제조사별 및/또는 브랜드별 및/또는 제품별로 상이하게 암호키를 할당한다. 예를 들어 주요 브랜드의 경우에는 동일한 브랜드를 사용하는 상품 종류별로 상이한 암호키를 사용하도록 결정할 수도 있다. 적은 수량만을 생산하는 회사의 경우에는 해당 제조사에 대해 단지 하나의 암호키만을 지정할 수도 있다.

<88> 판독기(20)에는 대상 제품의 태그를 읽는데 필요한 암호키들이 모두 구비된다. 암호화/복호화부(210)는 이동통신단말기로부터 제품 정보를 요청받으면, 암호키 특정정보(310)를 이동통신단말기로 송신하여 이동통신단말기가 자신이 저장하고 있는 암호키(330)와 동일한 암호키를 선택하도록 한다. 암호키 특정 정보(310)는 예를 들면 다수의 암호키에 부여된 인덱스일 수 있다. 이후에 암호화/복호화부(210)는 정보 제공부(250)가 외부로 전송하는 정보를 이 암호키로 암호화하며, 외부로부터 수신하여 입력되는 암호화된 메시지를 해독하여 정보 제공부(250)로 제공한다.

<89> 제 2 실시예에 있어서, 일부 암호키들이 유출되더라도 해당 업종 또는 해당 제조사 또는 해당 브랜드 또는 해당 제품으로 피해 범위가 제한된다. 또한 제 1 실시예와 마찬가지로 기존에 배포된 판독기를 업그레이드하지 않고도 동일한 암호키를 가지지만 새로운 제품정보를 저장한 새로운 많은 태그들을 추가로 편입하는 것이 가능하다. 나아가 제 2 실시예에 있어서, 충분한 수의 암호키를 이동통신단말기에 확보한다면, 여유분의 암호키를 할당함에 의해 보다 보안도가 높은 상태에서 새로운 제품을 편입하는 것이 가능하다. 즉, 새로운 태그(10)를 제작할

때 여유분으로 확보된 암호키 중 하나와 그에 대응되는 인덱스를 저장함에 의해, 판독기는 이 인덱스를 수신하여 여유분으로 확보된 암호키 중 하나를 그 태그를 위한 암호키로 특정하는 것이 가능하다.

<90> 본 발명에 따른 암호화/복호화부(210)의 제 3 실시예에 있어서, 태그의 저장부(300)에는 업종, 제조업체, 브랜드, 제품명 중의 적어도 2개의 기준에 따라 구분되어 할당된 적어도 2 개의 암호키들(330)과 이들 각각에 대응되는 암호키 특정정보들(310)이 저장된다.

<91> 도 6a는 이 같은 실시예에 따른 암호키(410)와 암호키 특정정보(420)의 일 예를 도시한다. 여기서 태그에 저장되는 암호키(410)는 3개의 암호키(411, 413, 415)로 구성되며, 각각의 암호키들은 업종, 제조사, 브랜드별로 정해진 것이다. 암호키 특정정보(420)는 암호키들과 각각 대응되는 인덱스 값들이다. 이동통신단말기(20)에는 모든 암호키들(433, 453, 473)과 이들 각각에 대응되는 암호키 특정정보로서의 인덱스들(431, 451, 471)이 저장된다. 이동통신단말기의 암호키들은 3 개의 그룹으로 구분되며, 각각의 그룹은 업종, 제조사, 브랜드별 암호키 할당 테이블이다. 예를 들면 이들 복수의 암호키들(411, 413, 415)은 3-DES 알고리즘에서 각 단계별로 사용되는 3 개의 암호키들일 수 있다.

<92> 태그(10)의 암호화/복호화부(210)는 이동통신단말기(20)로부터 제품 정보를 요청받으면, 암호키 특정정보(310)로서의 인덱스, 즉 여기서는 02, 01, 04의 값을 이동통신단말기로 송신한다. 이동통신단말기는 이 인덱스 값들로부터 대응되는 암호키 테이블들을 룩업하여 태그가 저장하고 있는 암호키(410)와 동일한 암호키 셋트, 즉 여기서는 1324, abcd, 2345를 현재 태그를 읽기 위한 암호키들로 선택하도록 한다. 이후에 태그(10)의 암호화/복호화부(210)는 이들 복수의 암호키들을 순차적으로 사용하여 이동통신단말기(20)와 송수신하는 정보들을 암호화 및 복호화한다.

<93> 본 발명의 유리한 양상에 따라 암호키가 특정되면 이동통신단말기는 이 암호키가 어느 특정한 업종, 제조업체, 브랜드에 속하는지, 또는 제품명이 무엇인지 알 수 있다. 즉, 도 6a에서 이동통신단말기는 수신한 암호키 인덱스들(421, 423, 425)로부터 현재 태그가 부착된 제품이 '악세서리' 업종에 속하며, 제조사가 '삼아공업'이고 브랜드명은 '가파찌'임을 알 수 있다. 따라서 제 3 실시예의 변형된 실시예에 있어서, 저장부(300)의 제품정보(370)와 암호키 특정정보(310) 정보는 실제로는 일부에 있어서 중복된 것일 수 있다. 즉, 인덱스들(421, 423, 425) 자체가 제품정보의 일부분일 수 있다.

<94> 제 3 실시예는 제 1, 2 실시예의 장점을 모두 가지며, 추가로 복수의 암호키들을 순차적으로 사용함에 의해 더욱 보안도를 높일 수 있고 새로운 제품 편입의 여유도 더욱 충분히 확보할 수 있다.

<95> 본 발명에 따른 암호화/복호화부(210)의 제 4 실시예에 있어서, 태그에는 복수의 암호키들(330)과 암호키 특정정보들(310)이 저장되고, 이동통신단말기(20)에는 모든 대상 제품의 제품 정보를 읽을 수 있도록 필요한 암호키들이 구비된다. 이 실시예에 있어서 태그는 이동통신단말기의 판독 요청을 받으면 다수의 암호키 중 하나를 선택하고 선택된 암호키에 해당하는 암호키 특정 정보를 이동통신단말기로 송신하여 상호간에 암호키를 일치시킨다. 태그의 암호키 선정은 예를 들면 로터리(rotary) 방식이나 난수(random) 방식에 의해 이루어진다. 이후에 태그는 선택된 암호키에 의해 이동통신단말기와 교환하는 정보를 암호화/복호화한다.

<96> 제 4 실시예는 제 1,2 실시예의 장점을 모두 가지며, 나아가 태그 자체가 암호키를 판독시마다 바꾸어 응답하므로 모조 판독기에 대한 대응력을 더욱 높일 수 있다.

<97> 본 발명에 따른 암호화/복호화부(210)의 제 5 실시예에 있어서, 태그에는 복수의 암호키 셋트들(330)과 암호키 특정정보 셋트들(310)이 저장되고, 이동통신단말기(20)에는 모든 대상 제품의 제품 정보를 읽을 수 있도록 필요한 암호키들이 구비된다. 태그측의 암호키 셋트들 각각은 업종, 제조업체, 브랜드, 제품명 중의 적어도 2개의 기준에 따라 구분되어 할당된 적어도 2 개의 암호키들을 포함한다. 예를 들면 이들 복수의 암호키들은 3-DES 알고리즘에서 각 단계별로 사용되는 3 개의 암호키들일 수 있다. 즉, 제 5 실시예에 있어서 태그에는 도 6a에 도시된 암호키들(411, 413, 415)이 복수 세트 저장되고, 암호키 특정정보들(421,423,425)도 복수 세트 저장된다.

<98> 암호화/복호화부(210)는 이동통신단말기와 통신하여 자신이 보유하고 있는 각각의 암호키들을 이동통신단말기가 특정하도록 한 후, 이들 복수의 암호키들을 순차적으로 사용하여 암호화 및 복호화를 처리한다. 태그의 암호키 선정은 예를 들면 로터리(rotary) 방식이나 난수(random) 방식에 의해 이루어진다. 이후에 태그는 선택된 암호키 세트에 의해 이동통신단말기와 교환하는 정보를 순차적으로 암호화/복호화한다.

<99> 제 3 실시예와 유사하게 제 5 실시예에 있어서도 암호키가 특정되면 이동통신단말기는 이 암호키가 어느 특정한 업종, 제조업체, 브랜드에 속하는지, 또는 제품명이 무엇인지 알 수 있다. 따라서 제 5 실시예의 변형된 실시예에 있어서, 저장부(300)의 제품정보(370)와 암호키 특정정보(310)는 실제로는 일부에 있어서 중복된 것일 수 있다.

<100> 제 5 실시예는 제 1 내지 제 4 실시예의 장점을 모두 가진다.

<101> 본 발명에 따른 암호화/복호화부(210)의 제 6 실시예에 있어서, 태그(10)에는 하나의 암호키와, 태그가 가진것과 동일한 암호키를 이동통신단말기측에서 생성하는데 필요한 암호키 생성 정보가 저장된다.

<102> 태그를 사용하는 회사들은 다수의 암호키를 준비하고, 예를 들면 업종별 및/또는 제조사별 및/또는 브랜드별 및/또는 제품별로 상이하게 암호키를 할당한다. 이동통신단말기(20)에는 대상 제품의 태그를 읽는데 필요한 모든 암호키들을 생성할 수 있는 암호키 생성모듈이 구비된다. 암호키 생성모듈은 하나 혹은 복수의 씨드(seed)값과 태그로부터 수신한 암호키 생성 정보로부터 암호키를 생성한다.

<103> 이동통신단말기에서 하나의 씨드값으로부터 생성될 수 있는 암호키의 수는 함수의 파라메터 값에 따라 무수히 많을 수 있다. 이동통신단말기에 비록 한정된 수의 씨드값만이 저장된 상태라 하더라도 판독기능을 업그레이드시키지 않고 무수히 많은 브랜드에 대해 서로 다른 암호키를 지정할 수 있다. 따라서 본 발명에 따른 정품 인증 장치는 이동통신단말기가 배포된 이후에도 판독기능을 업그레이드시키지 않고도 새로운 수많은 업종, 제조사, 브랜드 또는 제품을 인증 대상 제품에 편입시키는 것이 가능하다. 이는 새로운 암호키를 해당 제품에 지정하고 그 제품에 이 암호키를 생성할 수 있는 생성정보를 저장한 태그를 부착함에 의해 가능해진다. 더 나아가 본 발명에 따른 정품 인증 장치는 제품 정보값 표시부에 문장으로 표현되므로 동일한 암호키로도 다수의 종류의 제품에 대해 정품 인증을 하는 것이 가능하다.

<104> 암호키 생성모듈은 예를 들면 수신한 암호키 생성 정보로서의 정수 값 만큼 씨드(seed) 값을 거듭제곱한 값을 암호키로 생성할 수 있다. 그러나 본 발명은 이에 한정되지 않으며, 암호키 생성정보는 판독기에서 암호키를 특정하여 생성할 수 있는 정보를 포괄하도록 해석되어야 한다. 예를 들면, 암호키 생성정보는 제조사코드, 브랜드코드, 제품코드로 이루어진 일련의 코드열이나, 제조사명, 브랜드명, 제품명 등 으로 이루어진 텍스트 정보일 수도 있다. 또한 암호키 생성 알고리즘은 씨드값과 하나 이상의 파라메터로부터 암호키를 생성할 수 있는 수 많은 함수 및 연산을 포괄한다. 따라서 암호키 생성모듈의 생성 알고리즘을 적절히 선택함에 의

해 하나의 씨드값만을 판독기, 즉 이동통신단말기에 저장하고도 실질적으로 수많은 암호키들을 확보하는 것이 가능하다.

<105> 제 6 실시예에 있어서, 태그(10)의 암호화/복호화부(210)는 이동통신단말기(20)로부터 제품 정보를 요청받으면, 암호키 특정정보(310)로서 암호키 생성정보를 이동통신단말기로 송신하여 이동통신단말기가 자신이 저장하고 있는 암호키(330)와 동일한 암호키를 생성하도록 한다. 이후에 암호화/복호화부(210)는 정보 제공부(250)가 외부로 전송하는 정보를 이 암호키로 암호화하며, 외부로부터 수신하여 입력되는 암호화된 메시지를 해독하여 정보 제공부(250)로 제공한다.

<106> 이 실시예에 있어서, 암호키를 더욱 충분히 확보하여 업종, 제조사, 브랜드 또는 제품별로 충분히 많은 암호키를 할당함에 의해 일부 암호키가 유출된다하더라도 피해 범위를 최소로 하는 것이 가능하다. 또한 제 1 실시예와 마찬가지로 기존에 배포된 판독기를 업그레이드하지 않고도 동일한 암호키를 가지지만 새로운 제품정보를 저장한 새로운 많은 태그들을 추가로 편입하는 것이 가능하다. 나아가 이 실시예에 있어서 새로운 제품을 편입하고자 할 때 태그에 새로운 암호키와 그 암호키를 생성할 수 있는 암호키 생성정보만 저장한다면, 이동통신단말기는 저장한 씨드값과 태그로부터 수신한 암호키 특정정보에 의해 해당 태그가 보유한 것과 동일한 암호키를 생성할 수 있다. 따라서 보다 더욱 높은 보안 수준이 유지되면서 보다 많은 새로운 제품을 진품 인증 대상에 편입하는 것이 가능하다.

<107> 본 발명에 따른 암호화/복호화부(210)의 제 7 실시예에 있어서, 태그의 저장부(300)에는 업종, 제조업체, 브랜드, 제품명 중의 적어도 2개의 기준에 따라 구분되어 할당된 적어도 2개의 암호키들(330)과 이들 각각에 대응되는 암호키 특정정보(310)로서 암호키 생성정보들이 저장된다. 본 실시예에 있어서, 암호화/복호화부(210)는 저장된 암호키들을 순차적으로 사용

하여 메시지를 다중 암호화한다. 이동통신단말기는 태그로부터 암호키 생성정보를 수신하여 이 값과 내부의 씨드값을 기초로 특정한 함수나 연산을 통해 태그가 저장한 것과 동일한 세트의 암호키를 생성한다.

<108> 제 7 실시예는 제 6 실시예에 비해 복수의 암호키들에 의한 다중 암호화에 의해 더욱 보안도를 높일 수 있는 장점을 갖는다.

<109> 본 발명에 따른 암호화/복호화부(210)의 제 8 실시예에 있어서, 태그의 저장부(300)에는 업종, 제조업체, 브랜드, 제품명 중의 적어도 2개의 기준에 따라 구분되어 할당된 적어도 2개의 암호키들(330)과 이들 각각에 대응되는 암호키 생성정보들, 그리고 이들 암호키 생성정보를 특정하기 위한 식별정보로서 인덱스들이 저장된다. 본 실시예에 있어서, 암호화/복호화부(210)는 저장된 암호키들을 순차적으로 사용하여 메시지를 다중 암호화한다. 이동통신단말기는 태그로부터 암호키 생성정보에 대한 인덱스를 수신하여 이 값과 내부의 씨드값을 기초로 특정한 함수나 연산을 통해 태그가 저장한 것과 동일한 세트의 암호키를 생성한다.

<110> 도 6b는 이 같은 실시예에 따른 암호키(410)와 암호키 생성정보(420), 그리고 그 인덱스의 일 예를 도시한다. 도 6a와 대응되거나 동일한 구성은 동일한 도면부호로 표기하였다. 여기서 태그에 저장되는 암호키(410)는 3개의 암호키들(411, 413, 415)로 구성되며, 각각의 암호키들은 업종, 제조사, 브랜드별로 정해진 것이다. 예를 들면 이들 복수의 암호키들(411, 413, 415)은 3-DES 알고리즘에서 각 단계별로 사용되는 3 개의 암호키들일 수 있다. 이들 암호키들(411, 413, 415)을 생성할 수 있는 암호키 생성정보(490)로서 파라메터 값들(491,493,495)은 저장부(300)에 저장될 수도 있지만 반드시 필수적인 것은 아니다. 암호키 생성정보(490)를 특정하기 위한 인덱스값들(420)은 태그(10)의 저장부(300)에 저장되며, 이동통신단말기(20)가 암호키 특정을 요구하면 이동통신단말기(20)로 전송된다.

<111> 도 6b에서 암호키 '1324'(411)를 생성할 수 있는 암호키 생성정보는 '133'(491)이며, 이 암호키 생성정보를 식별하는 인덱스는 '02'(421)이다. 마찬가지로 암호키 'abcd'(413)와 암호키 생성정보 '256'(493), 그리고 인덱스 '01'(423)이 대응되며, 암호키 '2345'(415)와 암호키 생성정보 '267'(495), 그리고 인덱스 '04'(425)이 대응된다. 이동통신단말기의 암호키들은 3 개의 그룹으로 구분되며, 각각의 그룹은 업종, 제조사, 브랜드별 암호키 할당 테이블이다.

<112> 태그(10)의 암호화/복호화부(210)는 이동통신단말기(20)로부터 제품 정보를 요청받으면, 암호키 특정정보(310)로서의 인덱스, 즉 여기서는 '02', '01', '04'의 값을 이동통신단말기로 송신한다. 이동통신단말기는 이 인덱스 값들로부터 대응되는 암호키 테이블들을 룩업하여 태그가 저장하고 있는 암호키(410)와 동일한 암호키 셋트, 즉 여기서는 '1324', 'abcd', '2345'를 생성할 수 있는 암호키 생성정보, 즉 여기서는 '133', '256', '267'를 각각의 테이블의 암호키 생성정보 필드(433,453,473)에서 추출한다. 이동통신단말기는 이들 암호키 생성정보와 씨드값을 기초로 소정의 암호키 생성 알고리즘을 실행시켜 대응되는 암호키들을 생성하여 현재 태그를 읽기 위한 암호키들로 선택하도록 한다. 이후에 태그(10)의 암호화/복호화부(210)는 이들 복수의 암호키들을 순차적으로 사용하여 이동통신단말기(20)와 송수신하는 정보들을 암호화 및 복호화한다.

<113> 본 발명의 유리한 양상에 따라 암호키가 특정되면 이동통신단말기는 이 암호키가 어느 특정한 업종, 제조업체, 브랜드에 속하는지, 또는 제품명이 무엇인지 알 수 있다. 즉, 도 6b에서 이동통신단말기는 수신한 암호키 인덱스들(421, 423, 425)로부터 현재 태그가 부착된 제품이 '악세서리' 업종에 속하며, 제조사가 '삼아공업'이고 브랜드명은 '가파찌'임을 알 수 있다. 따라서 제 8 실시예의 변형된 실시예에 있어서, 저장부(300)의 제품정보(370)와 암호키 특

정정보(310) 정보는 실제로는 일부에 있어서 중복된 것일 수 있다. 즉, 인덱스들(421, 423, 425) 자체가 제품정보의 일부분일 수 있다.

<114> 제 8 실시예는 제 6,7 실시예의 장점을 모두 가지며, 나아가 인덱스를 송신하므로 보안도가 더 높아지는 외에 후술하는 바와 같이 이동통신단말기의 갱신이 용이하다는 장점을 갖는다.

<115> 이 같은 과정을 통해 이동통신단말기(20)는 해당 암호키를 특정하여 태그(10)에 저장된 제품정보를 요구하고 그 응답을 수신하여 표시부에 표시한다. 정당한 태그가 부착된 제품이라면 이동통신단말기와 태그간의 암호화/복호화 과정이 성공할 것이고 따라서 표시부에는 제품정보가 제대로 표시된다. 모조품이나 변조품이라면 암호화/복호화 과정이 실패하여 표시부에는 읽을 수 없는 무의미한 정보 혹은 모조품 경고가 표시될 것이다. 이에 의해 고객은 그 제품이 진품인지 여부를 확인할 수 있게 된다.

<116> 본 발명의 추가적인 유리한 양상에 따라 태그(10)의 제어부(200)는 유출 암호키 갱신부(220)를 포함할 수 있다. 유출 암호키 갱신부(220)는 약정된 암호키 중 하나 혹은 그 이상이 유출된 경우 모조 태그를 무력화시키기 위해 태그(10)측에 탑재되는 모듈이다. 이 모듈은 암호키 유출 사실이 적발된 후에 새로 제작되는 태그들에 탑재된다. 유출 암호키 갱신부(220)는 자신이 탑재된 태그를 읽고자 시도하는 이동통신단말기들에 대해 기존의 해당 암호키를 폐기하고 자신이 특정하는 새로운 암호키를 사용하도록 지시한다.

<117> 암호화/복호화부(210)의 제 1 실시예에 대응되는 유출 암호키 갱신부(220)의 실시예에 있어서, 새로 통용되어야 할 유일한 마스터키 자체가 이동통신단말기에게 전달된다. 이동통신단말기는 저장한 마스터키를 삭제하고 전달받은 마스터키를 새로운 암호키로 기록한다. 태그

와 이동통신단말기 간의 키 업그레이드 프로토콜을 적절히 정의함에 의해 마스터키의 해킹에 따른 위험을 감소시킬 수 있다.

<118> 암호화/복호화부(210)의 제 2 실시예에 대응되는 유출 암호키 갱신부(220)의 실시예에 있어서, 유출된 암호키와 동일한 업종 또는 제조사 또는 브랜드 또는 제품의 태그에 탑재되어 새로 통용되어야 할 해당 암호키가 이동통신단말기에게 전달된다. 이동통신단말기는 해당 태그에 대응되는 인덱스에 기존에 할당된 암호키를 폐기하고 새로 전달받은 암호키를 해당 업종 또는 제조사 또는 브랜드 또는 제품의 암호키로 저장한다.

<119> 암호화/복호화부(210)의 제 3 실시예에 대응되는 유출 암호키 갱신부(220)의 실시예에 있어서, 유출된 암호키와 동일한 업종, 제조사, 브랜드, 제품 등의 범주에 속하는 태그에 탑재되어 새로 통용되어야 할 해당 암호키들이 이동통신단말기에게 전달된다. 이동통신단말기는 각각의 범주별 테이블에서 해당 태그에 대해 할당된 인덱스에 대응되는 암호키를 새로 전달받은 암호키로 갱신한다. 예를 들어 도 6a에서 도시된 태그의 경우 브랜드 인덱스로 '04'가 지정되어 있는 바, 현재는 이에 대응되는 암호키로 '2345'가 할당되어 있지만 유출 암호키 갱신부(220)는 이를 예를 들면 '5678'로 갱신하도록 지시할 수 있다. 이는 직접 암호키를 전송해도 되지만 충분한 수의 미할당된 여유분의 암호키가 확보되어 있다면 여유분 암호키의 인덱스 중 하나를 지시함에 의해서도 가능하다. 예를 들어 '5678'에 대응되는 기존의 인덱스가 '15'라면 태그의 유출 암호키 갱신부(220)는 새로운 암호키 '5678'을 전송하는 대신 '15' 값을 전송하고, 이동통신단말기는 자신의 테이블에서 '15'에 대응되는 암호키 '5678'을 추출하여 이를 인덱스 '04'에 대응되는 암호키로 할당할 것이다. 결과적으로 이동통신단말기에서 인덱스 '04'와 '15'에는 동일한 암호키가 대응되게 된다.

<120> 암호화/복호화부(210)의 제 4 실시예에 대응되는 유출 암호키 갱신부(220)의 실시예에 있어서, 유출된 태그에 저장된 복수의 암호키들 중 유출된 암호키들이 갱신되어야 한다. 이동통신단말기는 암호키 테이블에서 유출된 암호키에 대응되는 인덱스에 저장된 암호키를 전달받은 새로운 암호키로 갱신한다.

<121> 암호화/복호화부(210)의 제 5 실시예에 대응되는 유출 암호키 갱신부(220)의 실시예에 있어서, 유출된 태그에 저장되는 복수의 암호키 세트들 전체가 갱신되어야 한다. 따라서 태그의 유출 암호키 갱신부(220)는 필요한 새로운 복수의 암호키 세트들 전체를 이동통신단말기로 전달하고 자신에 대응되는 암호키 세트들을 갱신하도록 요청한다. 이동통신단말기는 저장된 암호키 테이블에서 해당 태그에 할당된 암호키 세트들을 먼저 특정하고, 이후에 그 암호키 세트 전체를 전달받은 암호키들과 전달받은 순서대로 갱신한다.

<122> 암호화/복호화부(210)의 제 6 실시예에 대응되는 유출 암호키 갱신부(220)의 실시예에 있어서, 새로 통용되어야 할 암호키 생성 정보 자체가 이동통신단말기에게 전달된다. 이때 태그에는 새로운 암호키 생성정보에 대응되는 암호키가 저장된다. 이동통신단말기는 예를 들면 기존에 통용되던 암호키 생성 정보를 불량 태그로 블랙 리스트에 등록할 수 있다. 이 경우 이동통신단말기는 특정한 태그가 진위 인증을 요청하면 블랙 리스트와 제조 일자를 참조하여 좀 더 정확하게 모조 태그인지 여부를 판단할 수 있다. 따라서 특정한 제조 일자 이전에 제조된 태그는 동일한 암호키 생성 정보를 사용하더라도 진품으로 판단되고, 그 이후에 제조된 태그는 모조품으로 판단하는 것이 가능하다.

<123> 암호화/복호화부(210)의 제 7 실시예에 대응되는 유출 암호키 갱신부(220)의 실시예에 있어서, 새로 통용되어야 할 암호키 세트에 속한 암호키의 일부 혹은 전체가 유출될 수 있다. 유출 암호키 갱신부(220)는 유출된 암호키들에 대해 새로 통용되어야 할 암호키 생성 정보들을

이동통신단말기에게 전달한다. 이때 태그에는 새로운 암호키 생성정보들에 대응되는 암호키들이 저장된다. 이동통신단말기는 예를 들면 기존에 통용되던 암호키 생성 정보들을 불량 태그로 블랙 리스트에 등록할 수 있다.

<124> 암호화/복호화부(210)의 제 8 실시예에 대응되는 유출 암호키 갱신부(220)의 실시예에 있어서,새로 통용되어야 할 암호키 생성 정보들이 이동통신단말기에게 전달된다. 예를 들어도 6b에서 암호키 중 암호키 '1324'(411)가 유출되었다고 하자. 이때 새로 출고되는 태그에는 암호키 '1324' 대신에 새로운 암호키로 예를 들면 '1567'이 저장되고 이에 대응되는 암호키 생성정보로 예를 들면 '138'이 대응된다고 하자. 유출 암호키 갱신부(220)는 태그의 암호키 테이블(430)에서 원래 해당 태그에 할당된 인덱스인 '02'에 대응되는 암호키 생성정보인 '133'을 삭제하고 새로운 암호키 생성 정보인 '138'을 기록하도록 요청한다. 이에 따라 이후에는 이동통신단말기는 암호키 테이블(430)에서 인덱스 '02'에 대해 암호키 생성정보로 '138'을 추출할 것이고 이에 의해 암호키 '1567'을 생성할 것이다. 따라서 여전히 '1324'를 암호키로 갖고 있는 모조키나 기존에 판매된 태그에 대해서는 제품 정보의 판독이 불가능하여 모조품 판정을 내리게 된다.

<125> 본 발명의 추가적인 유리한 양상에 따라 태그(10)의 제어부(200)는 재전송 공격 차단부(230)를 포함할 수 있다. 암호화 기술에 있어서 재전송 공격은 로그인과 같은 암호화된 인증 절차에 있어서 유저가 전송하는 로그인 메시지 자체를 해킹하여 서버에 재전송함에 의해 서버로의 접속을 시도하는 공격을 의미한다. 이에 대한 대응책으로, 서버는 로그인을 요구하는 메시지에 난수를 포함시켜 암호화한 후 클라이언트로 전송하고, 클라이언트는 응답하는 로그인 메시지에 동일한 난수를 포함시킨다. 서버는 수신한 로그인 메시지를 인증할때 난수를 확인하

여 자신이 전송한 그 난수인 경우에만 로그인을 허용한다. 난수는 매번 랜덤하게 바뀌므로 이 같은 재전송 차단기술에 의해 동일한 로그인 메시지를 중복 사용하는 가능성은 차단된다.

<126> 본 발명은 이 같은 재전송 공격 차단 기술을 진품 인증에 도입한다. 이는 이동통신단말기가 판독을 요구하는 메시지나 태그가 응답하는 메시지 자체를 해킹하여 복제사용하는 것을 효과적으로 차단한다. 이에 따라 본 발명의 시스템에 대해 재전송 공격을 하는 것이 불가능하고 따라서 진품 인증은 한층 더 신뢰성을 가지는 것이 가능하다.

<127> 본 발명의 또다른 양상에 따라 태그(10)의 제어부(200)는 사후관리 처리부(270)를 포함할 수 있다. 태그(10)의 저장부에는 태그의 판독내역정보가 저장된다. 정보 제공부(250)는 매 판독시마다 예를 들면 판독기 일련번호, 판독일시와 같은 판독내역정보를 저장부(300)의 할당된 영역에 저장한다. 정보제공부(250)는 판독횟수를 관리하는 카운터 영역의 저장값이 소정치 이상인 경우에는 제품 정보를 제공하지 않지만, 사후관리 처리부(270)는 판독횟수에 관계없이 특정한 암호키를 갖고 로그인하는 특정 단말기, 즉 관리용 판독기에 대하여는 제품 정보뿐 아니라 판독내역정보까지 제공하도록 설계된다. 특정 판독기는 통상적인 판독기와 유사한 하드웨어로 구성되나, 이는 판매처에서 폐기되는 태그 또는 반품된 물건에 부착된 태그의 정보를 판독하여, 제품의 판매일시, 진품 인증한 사용자, 진품 인증한 일시 등의 정보를 알 수 있어 고객지향 마케팅의 사후 고객관리정보로 유용하게 활용할 수 있다.

<128> 본 발명의 또다른 유리한 양상에 따라 태그(10)의 제어부(200)는 리프레쉬(Refresh) 처리부(290)를 더 포함할 수 있다. 일반적으로 비휘발성 메모리는 기록 후 판독가능 횟수나 기간이 제한되며, 대략 10년 정도 동안만 데이터가 유지되는 것으로 알려져 있다. 그러나 예를 들어 각종 감정서나 골동품, 그림, 조각품과 같이 장기간 소장되는 제품의 경우에는 이 같은 기간이 너무 짧을 수 있다. 본 발명은 이러한 응용분야에 대응하여 태그에 리프레쉬(Refresh)

처리부(290)를 추가로 구비하여 판독할 때마다 데이터를 재기록하여 리프레쉬 처리한다. 리프레쉬하는 데이터는 암호키, 제품 정보와 카운터 값을 포함하여 메모리에 저장된 전체 데이터에 대해 수행되어야 한다. 이 경우 리프레쉬용 버퍼를 두고 일정한 크기의 블럭 별로 읽고 쓰기를 반복하여 처리할 수 있다. 이 같이 리프레쉬가 적용되는 제품의 경우에는 판독 가능 횟수를 아주 크게 하거나 또는 아예 제한하지 않는 것이 바람직하다.

<129> 이하에서는 본 발명의 바람직한 일 실시예에 따른 이동통신단말기(20)의 구성을 설명한다. 도 3은 본 발명의 바람직한 일 실시예에 따른 이동통신단말기(20)의 전체적인 구성을 개략적으로 도시한 블럭도이다. 본 발명의 바람직한 일 실시예에 따른 휴대용 태그판독기(20)는 이동 통신 단말기와 일체로 제공되며, 본 실시예에 있어서 조작부(930)와, 표시부(950)와, 배터리(미도시), 그리고 무선 통신망을 통해 서비스 관리 서버와 통신하는 무선 통신부(970)는 통상적인 이동 통신 단말기에서 제공되는 키패드와 액정 표시부, 배터리이다.

<130> 바람직한 일 실시예에 있어서, 이동통신단말기는 태그와 무선으로 데이터를 교환하고 필요한 전력을 무선으로 송출하는 태그통신부(500)와, 암호키/복호화 키들의 정보를 저장하는 저장부(910)와,

<131> 상기 조작부(930)로부터의 지시에 응답하여 태그측으로 제품정보를 요청하고 그로부터 수신한 제품정보를 상기 표시부에 표시하는 정보판독부(750)와, 태그통신부(500)와 송수신하는 정보를 암호화/복호화하는 암호화/복호화부(710)와, 정보 판독 내역을 상기 무선 통신부를 통해 송신하는 정보 전송부를 포함하는 제어부(700)를 포함하는 것을 특징으로 한다.

<132> 바람직한 일 실시예에 있어서, 조작부(930)는 통상적인 이동 통신 단말기의 키 버튼들에 추가하여 판독개시 버튼, 정보 전송 버튼과 같은 한 두개의 버튼을 더 포함한다. 표시부(950)

는 이동통신 단말기의 LCD를 이용한다. 무선통신부(970)는 이동 통신 기능을 제공하는 회로로, 예를 들면 CDMA 통신을 지원하는 Qualcomm사의 MSM계열 칩과 관련 RF회로가 될 수 있다.

<133> 태그통신부(500)는 안테나(510)와, 상기 안테나(510)를 통해 태그에서 필요한 전력을 무선으로 송출하는 전력 송출부(531)와, 수신되는 신호를 복조하는 복조부(533) 및 송신하는 신호를 변조하는 변조부(535)를 포함한다. 이들 구성은 태그의 비접촉식 통신수단(100)에 포함된 안테나(110), 전원공급부(131), 변조부(135), 복조부(133)에 대응되는 구성이므로 상세한 설명은 생략한다. 안테나(510)는 이동 통신 단말기의 표면 일 영역의 외주연을 따라 인쇄된 패턴으로 형성될 수 있다.

<134> 저장부(910)에는 전체 시스템을 제어하는 메인 프로그램과 정보 교환에 필요한 암호키를 생성하기 위한 씨드값(들)이 저장된다. 또다른 실시예에 있어서 저장부(910)에는 메인 프로그램과 정보 교환에 필요한 다수의 암호키들이 저장된다. 저장부(910)는 비휘발성 메모리, 예를 들면 ROM과, 임시기억장소인 RAM을 포함하여 구성될 수도 있고 단일의 플래시 메모리로 구성될 수도 있다. 저장부(910)에는 또한 이동통신단말기(20)가 판독한 태그들에 관한 정보인 판독내역정보를 저장한다.

<135> 제어부(700)는 통상적인 마이크로프로세서로 구현될 수 있다. 본 발명의 특징적인 양상에 따라 본 발명의 일 양상에 따른 이동통신단말기(20)의 제어부(700)는 조작부(930)로부터의 지시에 응답하여 태그측으로 제품정보를 요청하고 그로부터 수신한 제품정보를 상기 표시부에 표시하는 정보판독부(750)와, 태그통신부(500)와 송수신하는 정보를 암호화/복호화처리하는 암호화/복호화부(710), 그리고 정보 판독 내역을 상기 무선 통신부를 통해 송신하는 정보 전송부가 프로그램에 의해 소프트웨어적으로 구현된다.

<136> 정보판독부(750)는 태그의 정보제공부(250)와 상호 작용하며, 암호화/복호화부(710)는 태그측의 암호화/복호화부(210)와 상호작용하는 대응구성들이다. 정보판독부(750)는 태그로부터 수신한 제품 정보를 표시부(950)에 텍스트 또는 그래픽 형태로 표시한다. 정보 판독부(750)는 또한 실시간 클럭(Real Time Clock) 회로를 포함하여 현재 시각을 산출할 수도 있다. 정보 판독부(750)는 판독시마다 판독 시각 및 판독기의 일련 번호 등을 태그로 전송하여 판독 내역 정보의 일부로 저장되도록 한다.

<137> 본 발명의 특징적인 양상에 따른 일 실시예에 있어서, 암호화/복호화부(710)는 태그통신부(500)를 통해 태그로부터 암호키의 생성 정보를 수신하여 이 정보와 저장부(910)에 저장된 씨드값으로부터 암호키를 생성하고 이 암호키에 의해 암호화 및/또는 복호화를 처리한다.

<138> 바람직한 또다른 실시예에 있어서, 암호화/복호화부(710)는 태그측의 암호화/복호화부(210)와 통신하여 암호키 특정 정보를 수신하여 저장부(910)에 저장된 다수의 업체별 및/또는 브랜드별 및/또는 제품별 암호키들중 현재 판독중인 태그와 관련된 키들을 선택하고 이를 이용하여 두 기기간의 통신을 처리한다. 이 같은 통신 과정은 이후에 더 상세히 설명될 것이다.

<139> 이동통신단말기의 암호화/복호화부(710)는 태그의 암호화/복호화부(210)와 대응되는 것으로, 전술한 태그의 실시예들과 대응되는 구성이 가능하다.

<140> 이동통신단말기의 암호화/복호화부(710)의 가장 간단한 제 1 실시예는 태그의 암호화/복호화부(210)의 제 1 실시예에 대응된다. 이 실시예에 있어서, 저장부(910)에는 단지 하나의 암호키로서 마스터 키만이 저장된다. 암호화/복호화부(710)는 태그와 송수신하는 정보를 이에 의해 암호화/복호화한다. 이의 작용효과는 태그의 제 1 실시예에서 이미 설명하였다.

<141> 이동통신단말기의 암호화/복호화부(710)의 제 2 실시예는 태그의 암호화/복호화부 (210)의 제 2 실시예에 대응된다. 이 실시예에 있어서 저장부(910)에는 복수의 암호키가 인덱스들에 대응되어 저장된다. 암호화/복호화부(710)는 태그로부터 암호키 특정정보, 예를 들면 인덱스를 수신하여 암호키를 특정하고 이에 의해 태그와 송수신하는 정보를 암호화/복호화한다. 이의 작용효과는 태그의 제 2 실시예에서 이미 설명하였다.

<142> 이동통신단말기의 암호화/복호화부(710)의 제 3 실시예는 태그의 암호화/복호화부 (210)의 제 3 실시예에 대응된다. 이 실시예에서 있어서, 도 6a의 하단에 개념적으로 도시된 바와 같이, 각각의 분류, 즉 업종, 제조사, 브랜드, 제품명 등의 기준별로 암호키 테이블이 저장부(910)에 저장된다. 암호화/복호화부(710)는 태그로부터 복수의 암호키 특정정보로서 인덱스들을 수신하여 각각 대응되는 테이블에서 현재 태그를 위한 암호키 세트를 특정한다. 이후에 태그와 송수신하는 정보를 이들 암호키들에 의해 순차적으로 다중 암호화/복호화한다. 이의 작용효과는 태그의 제 3 실시예에서 이미 설명하였다.

<143> 판독기의 암호화/복호화부(710)의 제 4 실시예는 태그의 암호화/복호화부 (210)의 제 4 실시예에 대응된다. 이 실시예에서 있어서, 복수의 암호키들이 테이블로 저장부(910)에 저장된다. 암호화/복호화부(710)는 태그로부터 암호키 특정정보로서 인덱스를 수신하여 암호키 테이블을 룩업하여 현재 태그를 위한 암호키를 특정한다. 이후에 태그와 송수신하는 정보를 이들 암호키에 의해 암호화/복호화한다. 이의 작용효과는 태그의 제 4 실시예에서 이미 설명하였다.

<144> 판독기의 암호화/복호화부(710)의 제 5 실시예는 태그의 암호화/복호화부 (210)의 제 5 실시예에 대응된다. 이 실시예에서 있어서, 제 3 실시예와 유사하게 복수의 암호키 테이블들이 저장부(910)에 저장된다. 암호화/복호화부(710)는 태그로부터 암호키 특정정보로서 인덱스

를 수신하여 암호키 테이블들을 룩업하여 현재 태그를 위한 암호키 세트를 특정한다. 이후에 태그와 송수신하는 정보를 이들 암호키들에 의해 순차적으로 다중 암호화/복호화한다. 이의 작용효과는 태그의 제 5 실시예에서 이미 설명하였다.

<145> 이동통신단말기의 암호화/복호화부(710)의 제 6 실시예는 태그의 암호화/복호화부 (210)의 제 6 실시예에 대응된다. 이 실시예에서 있어서, 암호화/복호화부(710)는 암호키 생성 모듈을 포함한다. 암호키 생성 모듈에 필요한 씨드값은 저장부(910)의 데이터 영역에 저장될 수도 있고, 이 모듈의 프로그램 코드의 일부로 편입되어 저장될 수도 있다. 암호화/복호화부(710)는 태그로부터 수신한 암호키 생성정보 값으로 암호키 생성 모듈을 실행시켜 암호키를 생성하고, 이후에 태그와 송수신하는 정보를 이 암호키에 의해 암호화/복호화한다. 이의 작용효과는 태그의 제 6 실시예에서 이미 설명하였다.

<146> 이동통신단말기의 암호화/복호화부(710)의 제 7 실시예는 태그의 암호화/복호화부 (210)의 제 7 실시예에 대응된다. 이 실시예에서 있어서, 암호화/복호화부(710)는 암호키 생성 모듈을 포함한다. 암호키 생성 모듈에 필요한 씨드값은 저장부(910)의 데이터 영역에 저장될 수도 있고, 이 모듈의 프로그램 코드의 일부로 편입되어 저장될 수도 있다. 암호화/복호화부(710)는 태그로부터 수신한 암호키 생성정보 값들에의해 순차적으로 암호키 생성 모듈을 실행시켜 일련의 암호키들을 생성하고, 이후에 태그와 송수신하는 정보를 이 암호키들에 의해 순차적으로 다중 암호화/복호화한다. 이의 작용효과는 태그의 제 7 실시예에서 이미 설명하였다.

<147> 이동통신단말기의 암호화/복호화부(710)의 제 7 실시예는 태그의 암호화/복호화부 (210)의 제 7 실시예에 대응된다. 이 실시예에서 있어서, 암호화/복호화부(710)는 암호키 생성 모듈을 포함한다. 암호키 생성 모듈에 필요한 씨드값은 저장부(910)의 데이터 영역에 저장될 수도 있고, 이 모듈의 프로그램 코드의 일부로 편입되어 저장될 수도 있다. 암호화/복호화부

(710)는 태그로부터 수신한 암호키 생성정보 값들에의해 순차적으로 암호키 생성 모듈을 실행시켜 일련의 암호키들을 생성하고, 이후에 태그와 송수신하는 정보를 이 암호키들에 의해 순차적으로 다중 암호화/복호화한다. 이의 작용효과는 태그의 제 7 실시예에서 이미 설명하였다.

<148> 이동통신단말기의 암호화/복호화부(710)의 제 8 실시예는 태그의 암호화/복호화부 (210)의 제 8 실시예에 대응된다. 저장부(910)에는 도 6b의 하단에 개념적으로 도시한 바와 같은 테이블들이 저장된다. 암호화/복호화부(710)는 태그로부터 수신한 인덱스들로부터 암호키 테이블을 참조하여 암호키 생성정보 값들을 추출한다. 이후에 이들에의해 순차적으로 암호키 생성 모듈을 실행시켜 일련의 암호키들을 생성하고, 이후에 태그와 송수신하는 정보를 이 암호키들에 의해 순차적으로 다중 암호화/복호화한다. 이의 작용효과는 태그의 제 8 실시예에서 이미 설명하였다.

<149> 전술한 바와 같이 본 발명의 유리한 양상에 따라 이동통신단말기는 수신한 암호키 특정정보 또는 암호키 생성정보 또는 암호키 생성정보에 대한 인덱스로부터 해당 제품의 업종, 제조업체, 브랜드, 제품명 중 적어도 2개의 제품 정보를 특정하여 표시부에 표시하는 것이 가능하다. 이는 위의 실시예 중 적어도 제 3, 5, 7, 8 실시예에서 가능하다. 이동통신단말기의 저장부(910)에는 도 6a, 도 6b에 도시한 바와 같이 해당 암호키가 속한 분류별로 인덱스에 대응하여 제품 정보가 저장된다. 따라서 수신한 인덱스로부터 제품 정보의 적어도 일부를 특정하는 것이 가능하다.

<150> 본 발명의 또다른 특징적인 양상에 따라 본 발명의 일 실시예에 따른 이동통신단말기(20)의 제어부(700)는 정보 판독부(750)가 판독한 정보 판독 내역을 상기 무선 통신부를 통해 송신하는 정보 전송부(760)를 더 포함한다. 정보 전송부(760)는 정보 판독부(750)가 판독한 정보, 즉 업종, 제조업체, 브랜드, 제품명, 등급, 모델명, 생산지, 제조일, 일련번호 중의 하

나 혹은 그 이상의 제품 관련 정보와, 가격, 인증 시각 등의 정보 판독 내역 정보를 송신한다.

<151> 추가적으로 정보 전송부(760)는 진품 인증 후 구매 완료된 제품에 대한 구매 정보를 더 포함할 수 있다. 이동통신단말기 소지자는 조작부(930)의 진품 인증 키를 눌러 제품 정보를 표시부(950)에서 제품 정보를 확인하고 진품임을 확신한 후 거래를 진행시켜 제품을 구매한다. 구매 완료 후 조작부(930)의 구매 완료키를 누르면 최근 진품 인증된 제품들의 목록이 저장부(910)의 판독내역정보로부터 독출되어 표시부(950)에 표시된다. 사용자가 목록 중의 한 정보를 선택하여 확인키를 누르면 해당 제품이 구매 완료된 것으로 처리된다. 바람직한 일 실시예에 있어서, 구매 정보는 저장부(910)에서 취합된 후 조작부(930)에서 전송키를 누르면 일괄 전송된다. 정보 전송은 무선 통신부(970)를 통해 이루어지며, 무선 인터넷망을 통해 또는 단순히 단문 메시지로 전송될 수도 있다. 또다른 실시예에 있어서, 사용자가 구매 완료키를 누르면 그때 그때마다 구매 정보가 단문 메시지의 형태로 서비스 관리 서버(40)로 전송된다.

<152> 본 발명의 또다른 특징적인 양상에 따라 본 발명의 일 실시예에 따른 이동통신단말기(20)의 제어부(700)는 태그로부터 유출된 암호키에 대한 암호키 갱신 요구 정보를 수신하여 이로부터 상기 저장부에 기존에 저장된 해당 암호키를 폐기하고 새로 할당된 암호키로 갱신 처리하는 유출 암호키 갱신부(790)를 포함한다. 유출 암호키 갱신부(790)의 구체적인 실시예들 및 그 동작은 태그의 유출 암호키 갱신부(220)에서 이미 설명하였으므로 생략한다.

<153> 본 발명의 또다른 특징적인 양상에 따라 본 발명의 일 실시예에 따른 이동통신단말기(20)의 제어부(700)는 1회용 난수를 발생시켜 이를 송신할 정보에 부가하여 상기 암호화/복호화부로 공급하고, 그 응답으로 수신되는 정보에서 난수를 추출하여 동일성을 체크함에 의해 재전송 공격을 차단하는 재전송 공격 차단부(730)를 더 포함한다. 재전송 공격 차단부(730)는

태그(10)의 재전송 공격 차단부(230)와 대응되는 구성으로 동일한 기능을 하므로 상세한 설명은 생략한다.

<154> 본 발명의 또다른 특징적인 양상에 따라 본 발명의 일 실시예에 따른 이동통신단말기(20)의 제어부(700)는 외부의 다른 휴대용 태그판독기와 통신하여 서로를 인증하며, 그 인증결과정보를 상기 표시부(950)에 표시하는 판독기 인증부(770)를 더 포함할 수 있다. 이는 판독기 자체의 신뢰성을 상호 체크할 수 있도록 지원하는 기능이다. 판독기간의 인증 역시 태그통신부(500)를 통해 이루어지며, 이를 위해 특정한 암호키가 미리 정해진다. 암호화/복호화부(710)는 판독기간의 인증에 있어서도 동일한 동작을 한다. 재전송 공격 차단부(730)는 판독기간의 통신을 이용한 해킹을 차단하기 위해 이 과정에 개입하는 것이 바람직하다. 이의 동작에 대해서는 이후에 좀 더 상세히 설명한다.

<155> 본 발명의 또다른 특징적인 양상에 따라 본 발명의 일 실시예에 따른 이동통신단말기(20)의 제어부(700)는 비휘발성 메모리로 된 저장부의 암호키 관련정보를 읽은 후 읽은 정보를 재기록하는 리프레쉬(Refresh) 처리부를 더 포함한다.

<156> 바람직한 일 실시예에 있어서, 이동통신단말기(20)의 제어부(700)를 제어하는 메인 프로그램은 ROM과 같이 영구적으로 저장되는 기억소자를 사용한다. 그에 대해 암호키와 같은 정보는 ROM에 저장할 경우 복제될 위험이 있으므로 보안유지를 위해 플래시메모리에 저장된다. 플래시메모리의 경우 기록 후 판독 가능한 연한이 10년 정도로 제한되어 있으므로, 오랫동안 사용할 경우 암호키가 소실될 가능성이 있다. 본 발명의 일 실시예에 따른 이동통신단말기(20)는 암호키 정보 등 플래시 메모리에 저장된 정보를 읽을 때마다 읽은 데이터를 동일한 주소에 다시 재기록함에 의해 이 같은 문제점을 해결한다.

<157> 본 발명의 바람직한 일 실시예에 따른 태그판독기(20)는 휴대폰상에 구현된다. 이때 조작부(930)는 휴대폰의 키패드 중 하나 혹은 몇 개의 키를, 표시부(950)는 휴대폰의 액정 화면을 사용할 수 있다. 물론 저장부(910), 제어부(700)까지 휴대폰에서 기본적으로 탑재된 자체의 것을 사용할 수 있지만 이 경우 판독과 관련된 정보들이 유출될 위험이 있다. 이에 따라 본 발명의 바람직한 일 실시예에 따른 이동 통신 단말기는 별도로 설계된 ASIC을 내장하고 있다. 이 ASIC은 태그통신부(500)의 아날로그 무선 회로 및 변복조 회로는 물론, 자체에 저장부(910)로서의 불휘발성 메모리와 제어부(700)로서의 마이크로프로세서를 내장하고 있다. ASIC과 이동통신단말기의 시스템 제어용 마이크로프로세서는 각각의 호스트 인터페이스를 통해 통신한다. 이들 통신은 한정된 갯수의 명령만이 허용되므로 철저한 보안이 유지될 수 있다.

<158> 따라서 바람직한 일 실시예에 있어서 이동통신단말기는 별도로 설계된 ASIC과 단지 안테나 패턴의 구성만이 공지의 휴대폰에 추가됨으로써 본 발명에 따른 이동통신단말기의 하드웨어가 완성될 수 있다. 이때 이동통신 단말기에는 ASIC과의 통신과 사용자 인터페이스를 위한 별도의 소프트웨어 모듈이 추가로 설치되어야 한다.

<159> 이하에서는 본 발명에 따른 이동통신단말기와 태그 간의 통신 과정을 설명한다.

<160> 본 발명의 바람직한 일 실시예에 따른 이동통신단말기와 태그 간의 통신 과정은 :

<161> 업종, 제조업체, 브랜드, 제품명 중의 하나 또는 그 이상의 기준에 의해 암호키를 지정하고 그에 따른 암호키 관련 정보를 반도체 메모리에 저장하는 암호키 정보 저장 단계와, 비접촉식 태그의 존재를 검출하는 태그 검출 단계와, 상기 태그로부터 암호키의 특정을 위한 정보를 수신하여 이로부터 상기 반도체 메모리에 저장된 암호키 관련 정보로부터 암호키를 특정하여 현재 통신을 위한 암호키로 선택하는 암호키 특정 단계와, 상기 태그로 제품 정보를 요

청하는 정보 요구 메시지를 암호화하여 송신하는 제품 정보 요구 단계와, 수신한 브랜드명, 제품 이름, 등급 등을 포함하는 제품정보 메시지를 복호화하는 단계와, 상기 제품정보를 가시적인 정보로 표시하는 단계를 포함하는 것을 특징으로 한다.

<162> 본 발명의 추가적인 양상에 따르면, 바람직한 일 실시예에 있어서 상기 암호키 특정 단계는 태그로부터 수신한 암호키 생정 정보와 저장된 암호키 씨드 정보를 이용하여 암호키를 생성함에 의해 암호키를 특정함에 의해 암호키를 특정한다.

<163> 본 발명의 추가적인 양상에 따르면, 바람직한 일 실시예에 있어서 상기 제품정보 메시지를 복호화하는 단계는 상기 정보 제공 방법이 정보 요구 메시지를 암호화하는 단계 이전에 임의로 발생된 난수를 메시지에 포함시키는 단계와, 수신한 제품정보 메시지를 복호화한 후 난수의 동일성을 확인하여 재전송 공격에 대한 대응 처리를 실행하는 단계를 더 포함할 수 있다.

<164> 본 발명의 추가적인 양상에 따르면, 상기 정보 제공 방법이 유출된 암호키에 대한 폐기 및 새로운 암호키로의 갱신을 요구하는 암호키 갱신 요구 정보를 수신하는 단계와, 해당 제품에 대하여 기 지정된 암호키를 새로운 암호키로 대체하는 단계와, 상기 새로운 암호키를 현재 통신을 위한 암호키로 선택하는 단계를 더 포함하는 것을 특징으로 한다.

<165> 도 4는 본 발명의 일 실시예에 따른 태그(10)와 이동통신단말기(20)간의 통신 과정을 설명하는 도면이다. 이하에서는 도 4를 참조하여 이 같은 통신 과정을 보다 상세히 설명한다.

<166> 먼저 이동통신단말기에서 사용자가 특정한 버튼을 눌러 제품 정보의 확인을 요청한다(단계 S210). 이에 따라 이동통신단말기는 태그의 존재를 탐색한다(단계 S110). 이 같은 탐색 과정은 예를 들면 ISO14443 표준안에 규정된 것을 채택할 수 있으나 본 발명은 이에 한정되는 것은 아니다.

<167> 이후에 이동통신단말기는 선택적으로 암호키를 특정하는 프로토콜을 실행한다(단계 S132, S134). 태그에는 이동통신단말기와의 통신에 사용될 단지 하나의 암호키만이 저장되어 있을 수도 있고, 후술하는 프로토콜에 의해 그 중 하나가 특정되어 사용되는 복수의 암호키가 저장될 수도 있다.

<168> 먼저 이동통신단말기는 태그측으로 암호키의 특정을 요구한다(단계 S132). 암호키의 특정을 요구하는 메시지는 요청 메시지에 이동통신단말기측에서 발생한 난수를 부가하여 생성된다. 태그는 이에 대한 응답으로 암호키의 특정에 필요한 암호키 특정 정보, 예를 들면 인덱스를 송신한다(단계 S134). 이 특정 정보 메시지는 특정정보에 이동통신단말기측에서 송신한 난수를 부가하고, 새롭게 태그측에서 발생한 난수를 추가로 부가하여 생성된다. 이는 송신 메시지 뿐 아니라 수신 메시지도 재전송 공격으로부터 보호하기 위함이다. 바람직한 일 실시예에 있어어 암호화 방식은 3-DES 방식이며, 이 방식은 대칭키 방식이므로 암호화 키와 복호화 키가 동일하다.

<169> 또다른 실시예에 있어서, 암호키 특정 정보는 암호키 생성시 사용되는 암호키 생성 정보이다. 암호키 생성 정보는 일 실시예에 있어서 암호키 생성 함수에서 사용하는 파라메터 값이다. 이 실시예에 따른 이동통신단말기에는 암호키 생성 함수가 프로그램으로 구현되어 있다. 암호키 생성함수는 이동통신단말기의 저장부(910)에 저장된 씨드(seed) 값과 태그로부터 수신한 암호키 생성정보로부터 암호키를 생성한다(단계 S230). 예를 들어 간단한 실시 예에서 씨드값이 123456일 때 파라메터는 이들의 순열조합로부터 생성된 여러 개의 암호키 중 하나를 지정하는 인덱스일 수도 있다. 또 다른 실시 예에서 파라메터는 씨드값을 나타내는 데이터 워드를 블럭 단위로 스크램블링함에 의해 도출 가능한 수많은 암호키 중 하나를 지정하는 인덱스일 수도 있다. 또다른 실시예에서 파라메터는 씨드값을 나타내는 데이터 워드를 블럭 단위로 스

크램블링하는 알고리즘에서 블럭의 분할과 관련된 파라메터일 수도 있다. 이 같은 암호키 생성에 대해서는 다양한 방법이 공지되어 있으므로 상세한 설명은 생략한다.

<170> 판독기에 복수의 씨드값이 저장된 경우 태그에 저장되는 암호키 생성 정보는 씨드를 특정하는 인덱스를 포함하며, 나머지는 단일의 씨드를 가진 실시예와 유사하므로 상세한 설명은 생략한다.

<171> 이 같은 암호키 생성 함수를 활용함에 의해 본 발명은 판독기의 구입 이후에 판독기를 업그레이드시키지 않고도 제품별로 서로 상이한 암호키를 갖는 정품 인증 대상 상품을 적어도 생성 가능한 암호키의 수 만큼 추가할 수 있다.

<172> 또다른 실시 예에 있어서 암호키 특정 정보는 다수의 암호키 중 하나를 특정하는 인덱스이다. 이동통신단말기에는 모든 태그의 암호키에 대응되는 복수의, 예를 들면 수백개 정도의 암호키가 저장된다. 태그에는 자신의 암호키와 복수의 암호키 중 하나를 특정하는 인덱스가 저장된다. 이동통신단말기는 이 인덱스를 수신하여 다수의 암호키 중 현재 태그에 사용될 수 있는 하나의 암호키를 특정할 수 있다.

<173> 이 같이 복수의 암호키를 활용함에 의해 본 발명은 판독기의 구입 이후에 판독기를 업그레이드시키지 않고도 정품 인증 대상 상품을 적어도 암호키의 수 만큼 추가할 수 있다.

<174> 태그에 복수의 암호키가 저장되어 있는 실시예에 있어서, 암호키 특정 정보는 태그에 저장된 다수의 암호키를 특정하는 복수의 인덱스이다. 이동통신단말기는 수신한 복수의 인덱스 중 하나를 임의로 선택하여 응답한다. 이에 따라 태그측에서도 암호키의 특정이 이루어진다. 이 경우 이동통신단말기는 저장된 수많은 암호키 중 자신이 태그로부터 수신한 복수의 인덱스

중 임의로 선택한 하나의 인덱스에 해당하는 암호키가 현재 태그와의 마스터 키로 특정된다. 이에 의해 본 발명에따른 정품 인증 시스템은 한층 강화된 보안도를 구비할 수 있게 된다.

<175> 위의 3 가지 실시예에 있어서 암호키의 지정은 예를 들면 업종별 및/또는 제조사별 및/또는 브랜드별 및/또는 제품별로 이루어질 수 있다. 이에 의해 동일한 업종의 또는 동일한 업종의 동일한 제조사가 제조하는 제품들에 대해서는 동일한 암호키가 사용될 수도 있다. 이에 따라 동일한 업종 또는 동일한 업종의 동일한 제조사가 새로운 제품을 생산하여 본 발명에 따른 이동통신단말기에 의해 판독될 경우 이동통신단말기의 암호키 정보를 갱신하지 않고도 제품 정보를 읽을 수 있다. 나아가 동일한 종류의 제품에 대해 암호키를 공용할 경우 더욱 더 많은 수의 새로운 제품을 판독기 출시 이후에도 추가할 수 있다.

<176> 이후에 이동통신단말기(20)는 태그(10)로 제품 정보를 요청하는 메시지를 전송한다(단계 S152). 전술한 바와 같이 암호키 인덱스 또는 암호키 생성 정보 인덱스로부터 제품 정보의 일부가 미리 확보될 수도 있다. 이 메시지는 요청 메시지에 태그로부터 수신한 난수를 부가하고, 이동통신단말기측에서 새롭게 생성한 난수를 부가한 후 특정된 마스터 암호키로 암호화하여 생성된 메시지이다. 이 메시지를 수신한 태그는 수신한 제품 정보 요구 메시지에 포함되며, 이전에 자신이 송신한 난수를 추출하여 당초 송신한 난수와의 동일성을 확인하여 수신한 신호가 재전송 공격인지 여부를 체크할 수 있다. 이때 태그는 선택적으로(optionally) 이동통신단말기를 인증하는 과정을 추가로 실시할 수 있다. 이동통신단말기의 인증은 예를 들면 이동통신단말기에게 보내는 특정한 코드 메시지에 대한 응답 메시지를 수신하여 이를 해싱한 값을 체크함에 의해 이루어질 수 있다.

<177> 이후에 태그는 저장부(300)의 카운터 값을 추출하여 체크한다(단계 S330). 허용 가능한 횟수 이상으로 이미 판독이 완료된 태그라면 추가적인 판독이 차단되고, 그렇지 않다면 다음 단계로 이행한다.

<178> 이후에 태그는 제품 정보를 저장부(300)로부터 추출하여 응답 메시지를 생성한다(단계 S350). 이 메시지는 제품 정보에 이동통신단말기로부터 수신한 난수를 부가한 후 마스터 키로 암호화한 것이다. 생성된 제품 정보 메시지는 이동통신단말기로 전송된다(단계 S154). 태그는 이후에 저장부의 카운터 값을 증가시키고(단계 S370), 판독일시, 판독을 요청한 판독기 일련번호를 포함하는 판독 이력 정보를 저장부에 저장한다(단계 S390). 이동통신단말기는 이 메시지를 수신하여 복호화하고 복호화된 메시지 중에 포함된 난수를 당초 송신한 난수와 동일한지 확인하여 수신한 신호가 재전송 공격인지 여부를 체크한다(단계 S250). 재전송 공격에 의한 부정한 응답이 아니라고 판단되면 제품 정보를 표시한다(단계 S270).

<179> 이하에서는 태그와 이동통신단말기간의 유출 암호키에 대한 갱신 처리 절차에 대해 설명한다. 도4에서 이동통신단말기가 태그로 암호키의 특정요구 메시지를 송신하면(단계 S132), 태그는 암호키 특정 메시지를 송신하는 대신에 암호키 갱신요구 메시지를 송신한다(단계 S134). 이동통신단말기는 이 메시지를 수신하여 내부에 해당 태그에 대해 지정된 기존의 암호키를 폐기하고 새로운 암호키로 대체한다. 추가로 이동통신단말기는 갱신된 새로운 암호키를 현재 태그와의 통신을 위한 암호키로 특정한다. 이후의 과정은 동일하다.

<180> 도 5는 본 발명의 바람직한 일 실시예에 따른 판독기 혹은 이동통신단말기간의 인증 과정을 설명하는 도면이다. 도시된 바와 같이 먼저 두 판독기 중 하나의 판독기가 인증 과정에 있어서 마스터로 지정되어야 한다. 이 같은 지정은 사용자가 인증을 요구하는 버튼을 먼저 누

른 이동통신단말기가 마스터로 동작하도록 할 수도 있다(단계 S510). 마스터 판독기는 주위의 슬레이브 판독기의 존재를 탐색한다(단계 S412).

<181> 이 같이 마스터와 슬레이브가 정해지면 이후에 두 단말기간에 통신 세션을 개시하는 절차가 진행된다(단계 S414). 판독기간의 통신 세션은 마스터가 세션 식별자를 생성하고 이를 슬레이브로 전송하며, 두 판독기간의 통신이 동일한 세션 식별자를 포함하여 이루어짐에 의해 유지된다. 이에 의해 동일한 무선 주파수를 공용하는 환경에서도 특정한 접속(connection) 상태가 유지되거나 관리될 수 있다.

<182> 이후에 판독기간의 통신에 필요한 암호키를 할당하는 과정이 실행된다(단계 S432, S434). 이 과정은 태그와 판독기간의 마스터키 특정과정과 유사하다.

<183> 바람직한 일 실시예에 있어서 판독기간의 인증 절차는 전적으로 암호화에 의존한다. 즉, 정당한 판독기라면 정당한 암호키를 보유하고 있을 것으로 추정한다. 본 실시예에 있어서 인증 절차는 마스터 판독기가 특정한 메시지를 자신의 암호키로 암호화하여 슬레이브 판독기로 전송하면(단계 S452), 슬레이브 판독기가 이를 수신하여 복호화한 후 다시 암호화하여 전송한다(단계 S453). 이때 슬레이브 판독기는 체크 메시지를 수신하였음을 표시부에 표시할 수 있다(단계 S630).

<184> 이후에 마스터 판독기는 수신한 메시지를 복호화한 후 난수를 체크하여 재전송 공격인지 여부를 먼저 체크한다. 이후에 추출한 메시지가 당초 송신한 메시지와 동일한지를 체크하여 동일하다면 슬레이브 판독기는 정당한 암호키를 가진 판독기이고 그렇지 않다면 부정당한 판독기로 판단하여 그 결과를 표시한다(단계 S550). 그러나 본 발명은 이에 한정되지 않으며, 예를 들면 슬레이브 판독기가 수신한 메시지를 복호화한 후 약간의 메시지 가공, 예를 들면 수신

한 메시지에 미리 약정된 규칙에 따라 바이트 단위 또는 워드 단위로 매핑하여 응답할 수도 있다.

【발명의 효과】

<185> 이상에서 상세히 설명한 바와 같이 본 발명에 따른 진품 인증 장치는 소형이고 박형의 태그를 제공함에 의해 하나의 이동통신단말기로 의류, 신발류, 가죽제품류, 주류, 농수축산품, 의약품, 전자제품, 기계류제품 등 구매시에 진품 확인이 필요한 제품 뿐 아니라 귀금속류, 예술품과 같이 지속적이고도 장기적으로 진품 확인이 요구되는 제품까지, 더 나아가 감정서, 입장권, 각종 증명서 및 시설이용권, 금권, 유가증권, 중요서류 등 광범위한 종류의 물품들에 대해 진품 인증을 적용할 수 있다.

<186> 또한 본 발명에 따른 진품 확인 장치는 휴대폰 등의 형태로 휴대가 간편한 판독기를 제공함에 의해 어느 누구나 포켓 혹은 지갑에 판독기를 소지할 수 있다. 이에따라, 구매자 입장에서는 언제 어디서나 쉽고 간편하게 진품 여부를 확인할 수 있고, 판매자 입장에서는 언제, 어느 소비자에 의해 진품 여부를 인증하는 상황이 벌어질지 알 수 없어 모조품을 속여서 판매하려는 시도를 할 수 없게 된다. 더 나아가 이러한 휴대형 단말기가 대량으로 소비자에게 배포될 경우 판매자든 소비자든 가짜상품의 판매, 구매 경향 자체가 크게 위축될 것이다.

<187> 또한 본 발명에 따른 진품 인증 장치는 제품 정보가 이동통신단말기의 표시부에 평문으로 표시되므로 구매자가 그 결과를 직접 쉽게 확인할 수 있고 또한 깊은 신뢰감을 가지는 것이 가능하다.

<188> 또한 본 발명에 따른 진품 인증 장치는 진품의 인증 여부가 암호키의 유효성과 휴대형 단말기에 표시되는 내용을 사람의 육안에 의해 판단하는데 의존하므로

별도의 네트워크 접속이나 많은 분량의 데이터를 미리 추정 저장해야 하는 번거로움이 없다. 나아가 암호키가 동일하더라도 표시 내용에 의해 제품이 구별되므로 판독기 배포 이후에 새로이 출시되는 신제품 또는 다른 종류의 제품에 대해서도 동일한 암호키를 적용한다면 판독기를 업그레이드하지 않고도 진품 여부의 확인이 가능하다.

<189> 또한 본 발명에 따른 진품 인증 장치는 판독기 혹은 이동통신단말기에 수많은 암호키를 생성할 수 있는 암호키 생성 모듈을 내장하거나 암호키를 복수개 저장함에 따라 한정된 메모리로도 수많은 암호키를 확보하는 것이 가능하여, 이미 판독기를 취득한 이후에도 더욱 더 수많은 업체, 브랜드 또는 제품에 대해 새로운 암호키를 부여하여 진품 인증 대상에 추가하는 것이 가능하다.

<190> 나아가 일부 업체, 브랜드 또는 제품의 암호키가 유출된 경우에도 나머지 업체, 브랜드 또는 제품에 대해서는 암호키가 달라 보안이 유지될 수 있고, 암호키가 유출된 경우에는 새로운 암호키를 할당함으로써 추가로 출고되는 제품에 대해서는 모조 판독기의 사용을 막을 수 있는 여지를 더욱 충분히 확보할 수 있게 된다.

<191> 이에 따라 본 발명은 이미 배포된 수많은 판독기를 업그레이드해야 새로운 제품에 적용할 수 있는 종래 기술에 비해 훨씬 유리한 장점을 가진다.

<192> 또한 본 발명에 따른 진품 인증 장치는 판독 횟수를 제한함에 의해 태그를 손상시키지 않고도 태그의 재사용을 방지할 수 있을 뿐만 아니라, 나아가 물리적인 방법에 비해 훨씬 신뢰성 있게 재사용되어서는 안될 태그들이 모조품에 재 활용되는 것을 차단할 수 있다.

<193> 또한 본 발명에 따른 진품 인증 장치는 골동품이나 예술품과 같이 소장 기간이 장기간인 제품에 대해 전자적인 메모리의 데이터 보존 연한 한계를 매 판독 시마다 메모리 리프레쉬

과정을 실행함에 의해 보존년한의 한계를 극복하여 적용 대상 물품의 범위를 더욱 넓힐 수 있다.

<194> 또한 본 발명에 따른 진품 인증 장치는 재전송 공격에 대해 대응함에 의해 진품 인증 메시지를 해킹하여 본 인증 시스템 자체를 복사하려는 시도를 차단하고 진품 인증의 신뢰성을 한층 더 높일 수 있다.

<195> 또한 본 발명에 따른 진품 인증 장치는 일부 암호키가 유출될 경우 새롭게 발행되는 태그를 통해 이동통신단말기를 오프라인 상에서 업그레이드하므로 사용자 입장에서는 아무런 조작도 없이 판독기가 업그레이드되는 장점이 있을 뿐 아니라 모조품의 등장에 따른 피해를 최소화할 수 있는 잇점이 있다.

<196> 또한 본 발명에 따른 진품 인증 장치는 휴대형 태그판독기간에 상호 인증이 가능하므로, 모조 비접촉식 통신 태그를 대상으로 동작하는 모조 휴대형 판독기가 사용되는 것도 방지할 수 있다.

<197> 또한 본 발명에 따른 진품 인증 장치는 이동 통신망을 통해 판독 내역 정보를 서비스 관리 서버에서 취합하는 것이 가능하고 취합된 정보를 제품 제조사에게 제공하여 유용한 마케팅 정보로 활용하는 것이 가능하다.

<198> 이제까지 본 발명은 바람직한 실시예들을 참조하여 설명되었지만 여기에 한정되는 것은 아니다. 따라서 본 발명은 본 발명의 범주를 벗어남이 없이 당업자라면 자명하게 도출가능한 많은 변형예들을 포괄하도록 의도된 첨부된 특허청구범위에 의하여 해석되어져야 한다.

【특허청구범위】

【청구항 1】

제품에 설치되어 그 제품의 정보를 제공하는 비접촉식 통신 태그를 판독하는 이동통신단말기에 있어서,

조작부와 ; 표시부와;

태그와 무선으로 데이터를 교환하고 필요한 전력을 무선으로 송출하는 태그통신부와;

무선 통신망을 통해 서비스 관리 서버와 통신하는 무선통신부와;

암호키 관련 정보를 저장하는 저장부와;

상기 조작부로부터의 지시에 응답하여 태그측으로 제품정보를 요청하고 그로부터 수신한 제품정보를 상기 표시부에 표시하는 정보판독부와, 상기 태그통신부를 통해 송수신하는 정보를 암호화/복호화하는 암호화/복호화부와, 정보판독 내역을 상기 무선통신부를 통해 송신하는 정보전송부를 포함하는 제어부;를 포함하는 것을 특징으로 하는 이동통신단말기.

【청구항 2】

제 1 항에 있어서, 상기 태그통신부가 :

안테나와, 상기 안테나를 통해 태그에서 필요한 전력을 무선으로 송출하는 전력 송출부와, 수신되는 신호를 복조하는 복조부 및 송신하는 신호를 변조하는 변조부를 포함하는 것을 특징으로 하는 이동통신단말기.

【청구항 3】

제 2 항에 있어서, 상기 정보전송부가 :

상기 조작부의 구매확인키가 눌러지면 구매 정보를 상기 정보판독 내역의 일부로 포함하여 송신하는 것을 특징으로 하는 이동통신단말기.

【청구항 4】

제 2 항에 있어서, 상기 정보전송부가 :

매 판독시마다 정보판독내역을 상기 저장부에 저장하였다가 상기 조작부의 전송키가 눌러지면 저장된 정보판독 내역을 일괄 송신하는 것을 특징으로 하는 이동통신단말기.

【청구항 5】

제 3 항에 있어서,

상기 저장부가 다수의 암호키를 저장하고,

상기 암호화/복호화부가 상기 무선통신부를 통해 태그로부터 암호키 특정 정보를 수신하여 이로부터 특정된 암호키에 의해 암호화/복호화를 처리하는 것을 특징으로 하는 이동통신단말기.

【청구항 6】

제 5 항에 있어서,

상기 저장부가 업종, 제조업체, 브랜드, 제품명 중 적어도 2개의 기준들의 각각에 대해 복수의 암호키들을 저장하고,

상기 암호화/복호화부는 상기 무선통신부를 통해 태그로부터 각각의 기준별로 암호키 특정 정보를 수신하여 이로부터 특정된 암호키들에 의해 암호화/복호화를 처리하는 것을 특징으로 하는 이동통신단말기.

【청구항 7】

제 4 항에 있어서,

상기 저장부가 다수의 암호키를 저장하고,

상기 암호화/복호화부가 상기 무선통신부를 통해 태그로부터 암호키 특정 정보를 수신하여 이로부터 특정된 암호키에 의해 암호화/복호화를 처리하는 것을 특징으로 하는 이동통신단말기.

【청구항 8】

제 7 항에 있어서,

상기 저장부가 업종, 제조업체, 브랜드, 제품명 중 적어도 2개의 기준들의 각각에 대해 복수의 암호키들을 저장하고,

상기 암호화/복호화부는 상기 무선통신부를 통해 태그로부터 각각의 기준별로 암호키 특정 정보를 수신하여 이로부터 특정된 암호키들에 의해 암호화/복호화를 처리하는 것을 특징으로 하는 이동통신단말기.

【청구항 9】

제 3 항에 있어서,

상기 저장부가 다수의 암호키들을 생성하기 위한 적어도 하나의 씨드값을 저장하고,

상기 암호화/복호화부가 상기 무선통신부를 통해 태그로부터 암호키의 생성 정보를 수신하여 이 정보와 상기 씨드값으로부터 암호키를 생성하고 이 암호키에 의해 암호화 및/또는 복호화를 처리하는 것을 특징으로 하는 이동통신단말기.

【청구항 10】

제 9 항에 있어서,

상기 저장부가 업종, 제조업체, 브랜드, 제품명 중 적어도 2개의 기준들의 각각에 대한 복수의 암호키들을 생성하기 위한 하나 또는 다수의 씨드(seed)값을 저장하고,

상기 암호화/복호화부는 상기 무선통신부를 통해 태그와 각각의 기준별로 암호키 생성 정보를 수신하여 이로부터 생성된 암호키들에 의해 암호화/복호화를 처리하는 것을 특징으로 하는 이동통신단말기.

【청구항 11】

제 4 항에 있어서,

상기 저장부가 다수의 암호키들을 생성하기 위한 적어도 하나의 씨드값을 저장하고,

상기 암호화/복호화부가 상기 무선통신부를 통해 태그로부터 암호키의 생성 정보를 수신하여 이 정보와 상기 씨드값으로부터 암호키를 생성하고 이 암호키에 의해 암호화 및/또는 복호화를 처리하는 것을 특징으로 하는 이동통신단말기.

【청구항 12】

제 11 항에 있어서,

상기 저장부가 업종, 제조업체, 브랜드, 제품명 중 적어도 2개의 기준들의 각각에 대한 복수의 암호키들을 생성하기 위한 하나 또는 다수의 씨드(seed)값을 저장하고,

상기 암호화/복호화부는 상기 무선통신부를 통해 태그와 각각의 기준별로 암호키 생성 정보를 수신하여 이로부터 생성된 암호키들에 의해 암호화/복호화를 처리하는 것을 특징으로 하는 이동통신단말기.

【청구항 13】

제 1 항 내지 제 12 항 중의 어느 한 항에 있어서, 상기 제어부가 :

태그가 송신한 유출된 암호키에 대한 암호키 갱신 요구 정보를 수신하여 그에 따라 상기 저장부에 기존에 저장된 해당 암호키를 폐기하고 새로 할당된 암호키로 갱신 처리하는 유출 암호키 갱신부를 더 포함하는 것을 특징으로 하는 이동통신단말기.

【청구항 14】

제 1 항 내지 제 12 항 중의 어느 한 항에 있어서, 상기 제어부가 :

1회용 난수를 발생시켜 이를 송신할 정보에 부가하여 상기 암호화/복호화부로 공급하고, 그 응답으로 수신되는 정보에서 난수를 추출하여 동일성을 체크함에 의해 재전송 공격을 차단하는 재전송 공격 차단부;를 더 포함하는 것을 특징으로 하는 이동통신단말기.

【청구항 15】

제 1 항 내지 제 12 항 중의 어느 한 항에 있어서, 상기 제어부가 :

외부의 다른 휴대용 태그판독기능을 가진 이동통신단말기와 통신하여 서로를 인증하며, 그 인증결과정보를 상기 표시부에 표시하는 판독기 인증부를 더 포함하는 것을 특징으로 하는 이동통신단말기.

【청구항 16】

제 1 항 내지 제 12 항 중의 어느 한 항에 있어서,

상기 저장부가 비휘발성 메모리로 구성되고,

상기 제어부가 상기 저장부의 정보를 읽은 후 읽은 정보를 재기록하는 리프레쉬(Refresh) 처리부를 더 포함하는 것을 특징으로 하는 이동통신단말기.

【청구항 17】

제 1 항 내지 제 12 항 중의 어느 한 항에 있어서, 상기 제어부, 저장부, 무선통신부의 알에프 회로가 하나의 ASIC으로 구현되고, 상기 제어부는 이동통신 단말기의 시스템 제어용 마이크로프로세서와 호스트 인터페이스를 통해 통신하는 것을 특징으로 하는 이동통신단말기.

【청구항 18】

이동 통신사의 가입자 서버와 네트워크를 통해 통신 가능하고 다수의 이동통신단말기와 이동통신망을 통해 통신 가능한 진품 인증 서비스 관리 서버에 의해 실행 가능한 진품 인증 서비스 관리 방법에 있어서, 상기 방법이 :

이동 통신 단말기로부터 판독 대상 제품마다 고유하게 할당된 제품 고유번호 및 이동통신 단말기마다 고유하게 할당된 판독기 고유번호를 포함하는 제품 정보 판독 내역 정보를 수신하는 단계와;

상기 수신한 내역 정보에 포함된 이동 통신 단말기의 식별번호로부터 상기 가입자 서버로 조회하여 가입자 정보를 수신받는 단계와;

상기 수신한 내역 정보와 상기 수신한 가입자 정보로부터 가입자의 분류정보와 제품 정보 판독 내역 정보를 취합하여 고객관리 정보로 저장하는 단계와;

출력 요구에 응답하여 상기 고객관리 정보를 보고서로 생성하여 출력하는 단계;

를 포함하는 것을 특징으로 하는 진품 인증 서비스 관리 방법.

【청구항 19】

제 18 항에 있어서,

상기 분류정보가 가입자의 연령, 지역, 성별, 직업 중의 복수의 정보를 포함하고,

상기 진품 인증 내역 정보가 업종, 제조업체, 브랜드, 등급, 모델명, 생산지, 제조일, 일련번호, 가격, 인증 시각 중의 복수의 정보를 포함하는 것을 특징으로 하는 진품 인증 서비스 관리 방법.

【청구항 20】

제 19 항에 있어서, 상기 진품 인증 내역 정보가 구매 완료된 제품에 대한 구매가격과 구매일시를 포함하는 구매 정보를 더 포함하는 것을 특징으로 하는 진품 인증 서비스 관리 방법.

【청구항 21】

제 18 내지 20 항 중의 어느 한 항에 있어서, 상기 고객관리 정보가 포인트 정보를 더 포함하고,

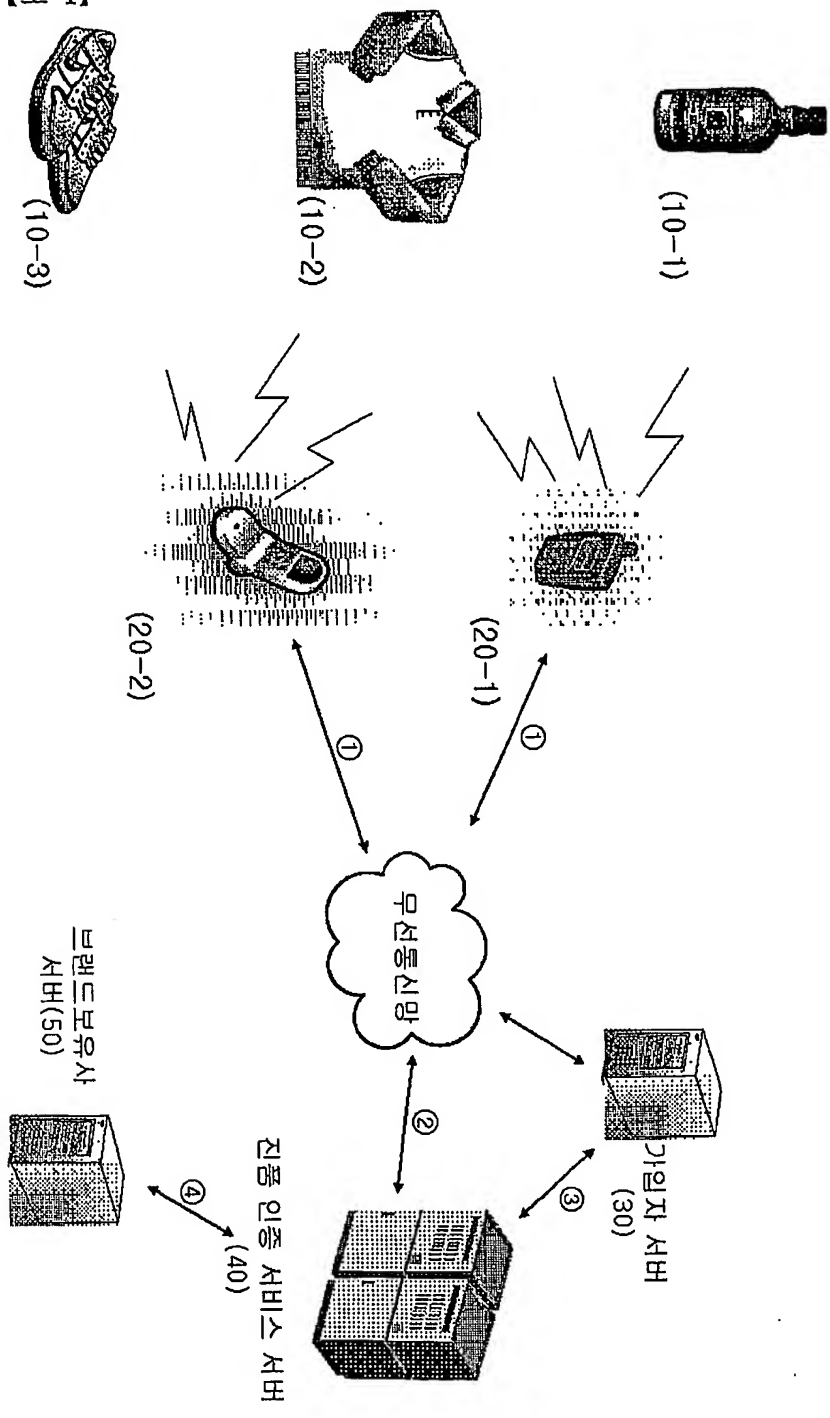
상기 서비스 관리 방법이 상기 수신한 진품 인증 내역 정보에 따라 해당 가입자의 포인트를 가산하는 단계를 더 포함하는 것을 특징으로 하는 진품 인증 서비스 관리 방법.

【청구항 22】

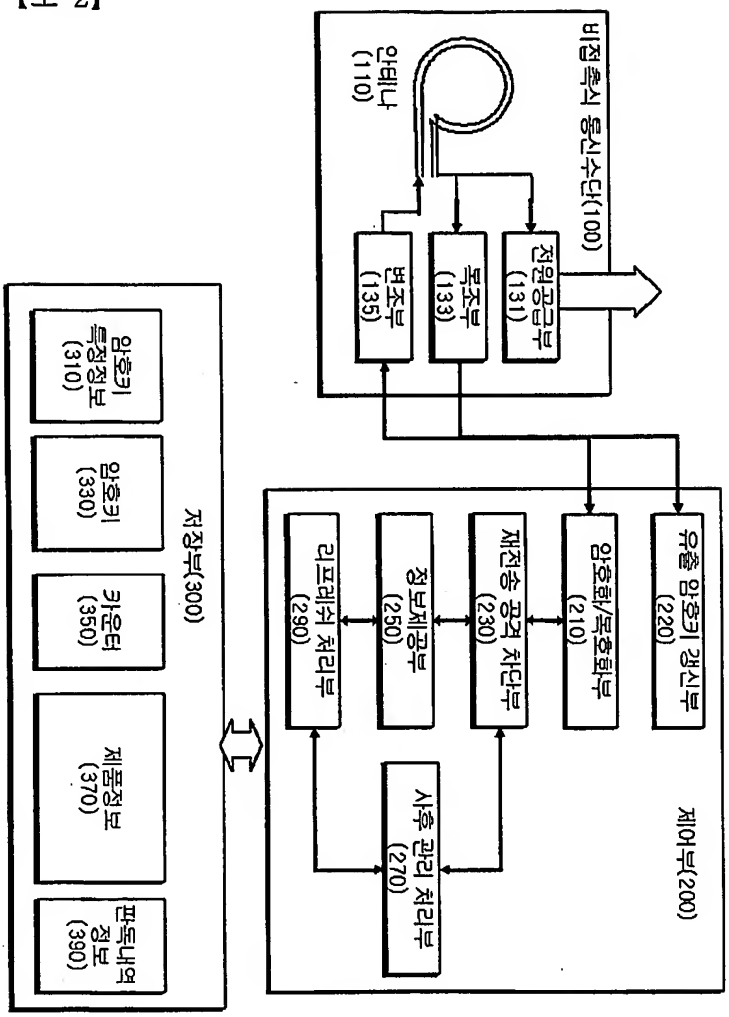
제 21 항에 있어서, 상기 서비스 관리 방법이 제품 정보 판독 내역 정보를 수신하는 단계 이후에 판독 내역 정보에 포함된 제품 정보 고유번호 및 판독기 고유번호가 이전에 수신한 제품 정보 판독 내역 정보와 동일한지를 체크하여 재전송된 내역 정보인지를 체크하는 단계를 더 포함하는 것을 특징으로 하는 진품 인증 서비스 관리 방법.

【도면】

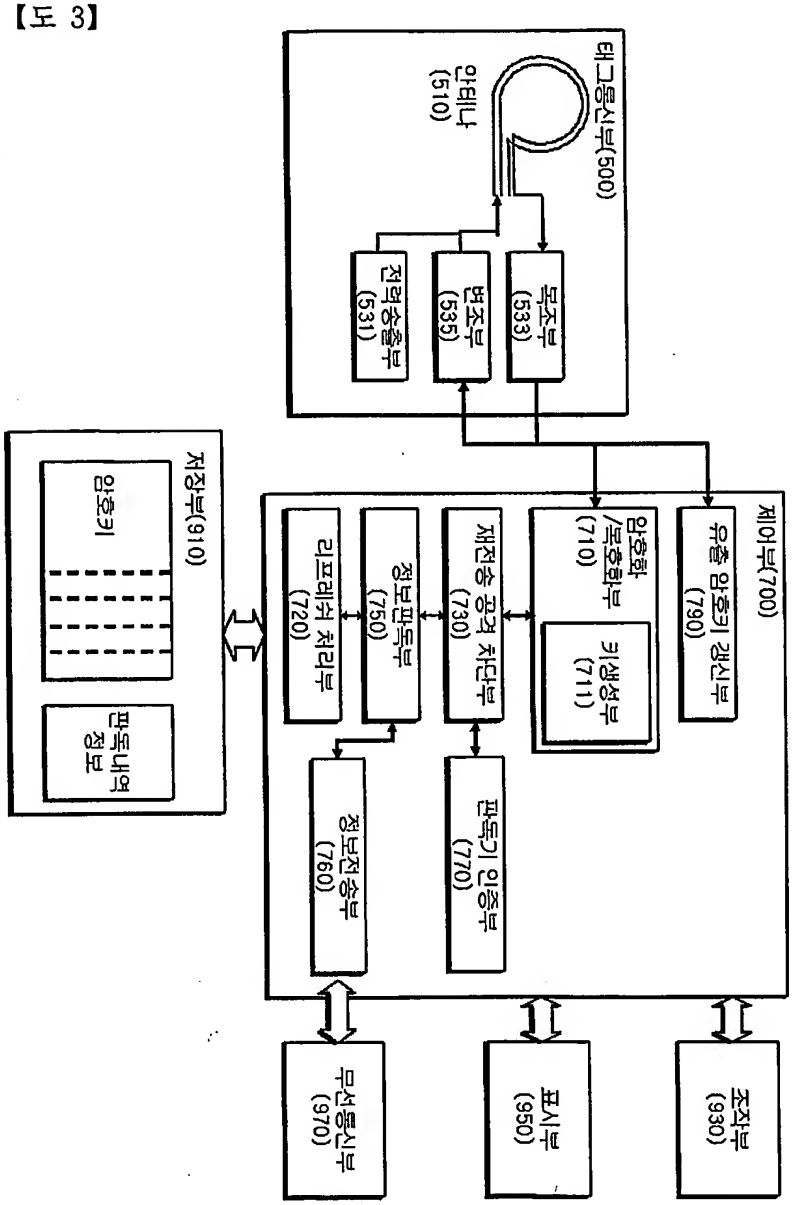
【도 1】


(10-3)
(10-2)
(10-1)
(20-2)
(20-1)
①
①
무선통신망
②
③
④
브랜드보유사 서버(50)
진품 인증 서비스 서버 (40)
가입자 서버 (30)

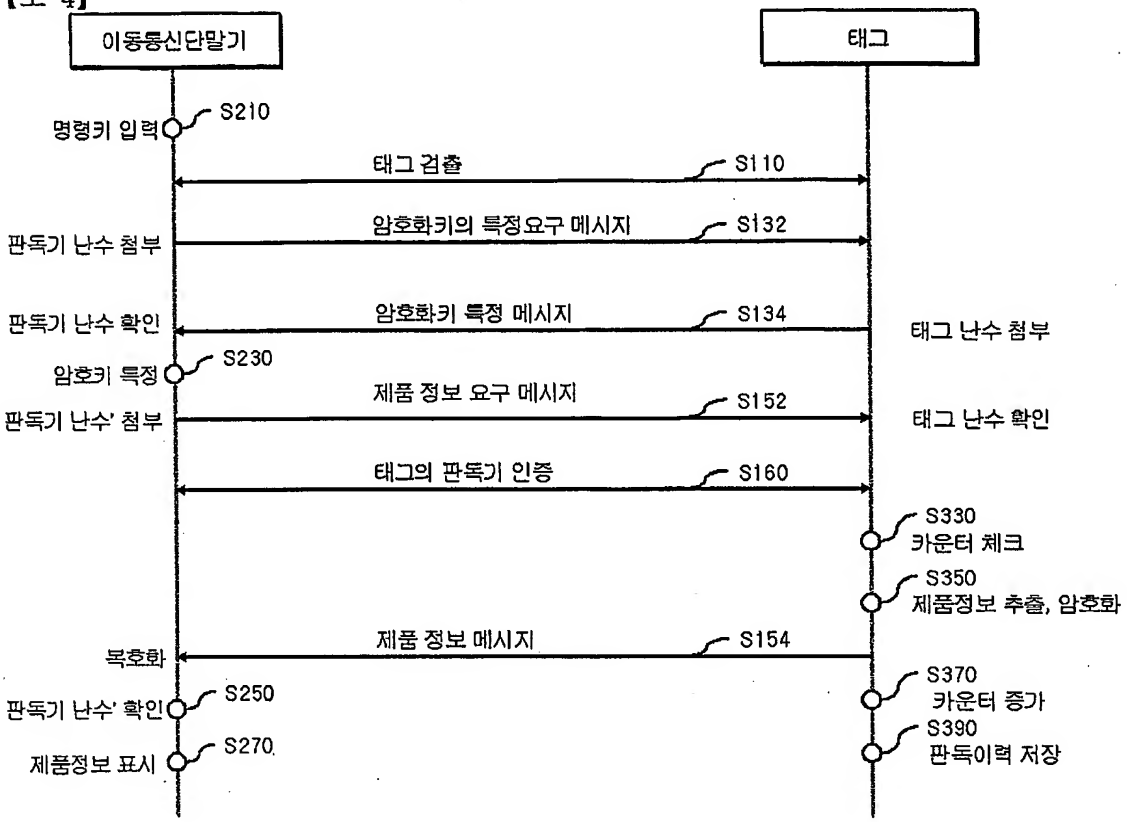
【도 2】


비접촉식 통신수단(100)
안테나 (110)
변조부 (135)
복조부 (133)
전원공급부 (131)
제어부(200)
유출 암호키 갱신부 (220)
암호화/복호화부 (210)
재전송 공격 차단부 (230)
정보제공부 (250)
리프레쉬 처리부 (290)
사후 관리 처리부 (270)
저장부(300)
암호키 특정정보 (310)
암호키 (330)
카운터 (350)
제품정보 (370)
판독내역 정보 (390)

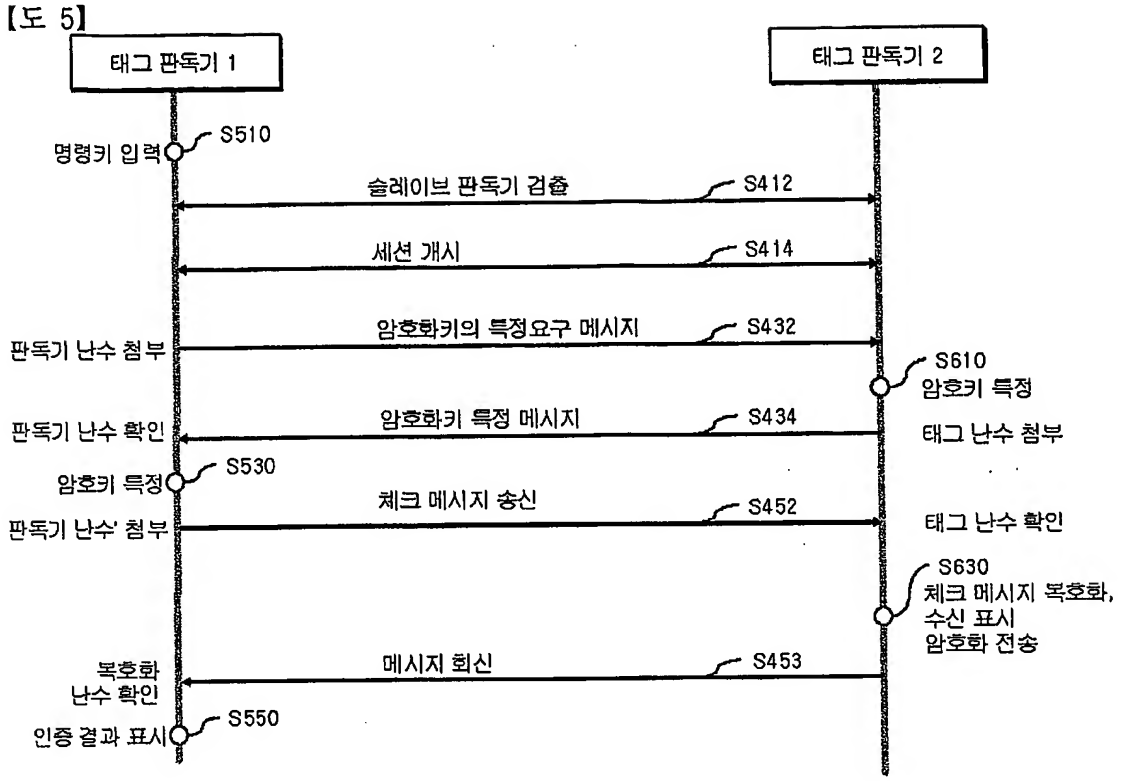
【도 3】


태그통신부(500)
안테나 (510)
전력송출부 (531)
변조부 (535)
복조부 (533)
저장부(910)
암호키
판독내역 정보
제어부(700)
리프레쉬 처리부 (720)
정보판독부 (750)
재전송 공격 차단부 (730)
암호화 /복호화부 (710)
키생성부 (711)
유출 암호키 갱신부 (790)
정보전송부 (760)
판독기 인증부 (770)
무선통신부 (970)
표시부 (950)
조작부 (930)

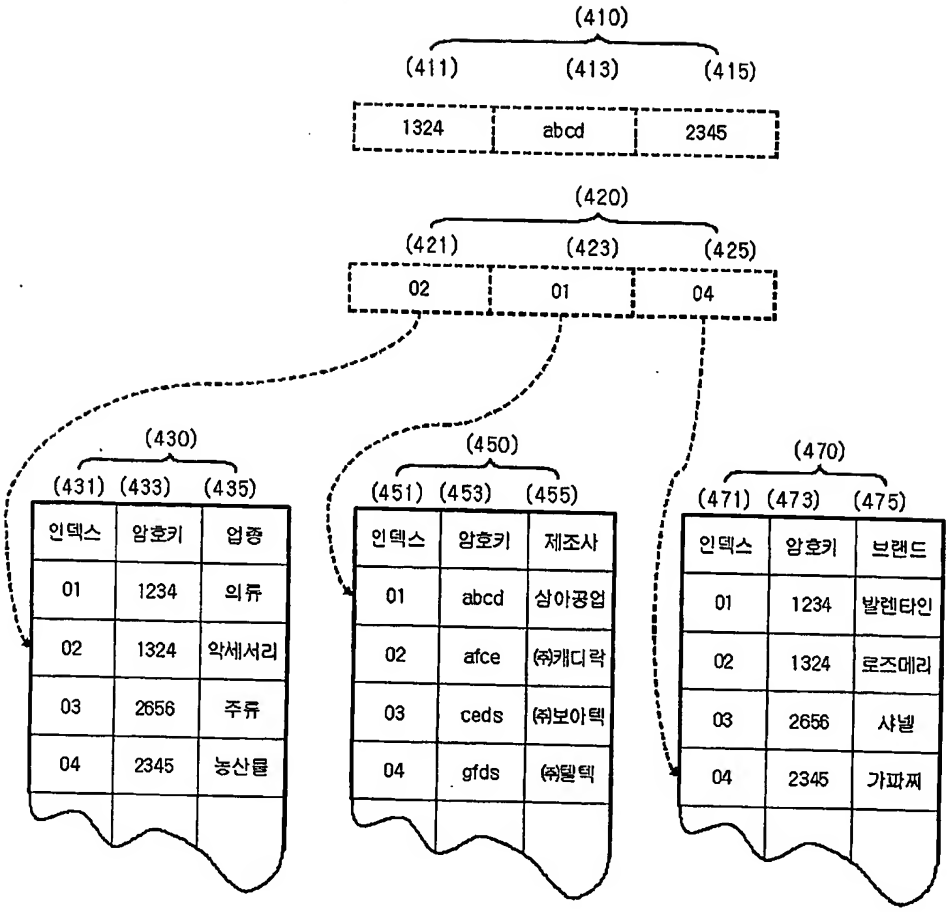
【도 4】


이동통신단말기
태그
S210
명령키 입력
태그 검출
S110
암호화키의 특정요구 메시지
S132
판독기 난수 첨부
판독기 난수 확인
암호화키 특정 메시지
S134
태그 난수 첨부
S230
암호키 특정
제품 정보 요구 메시지
S152
판독기 난수' 첨부
태그 난수 확인
태그의 판독기 인증
S160
S330
카운터 체크
S350
제품정보 추출, 암호화
제품 정보 메시지
S154
복호화
S370
카운터 증가
S250
판독기 난수' 확인
S390
판독이력 저장
S270
제품정보 표시

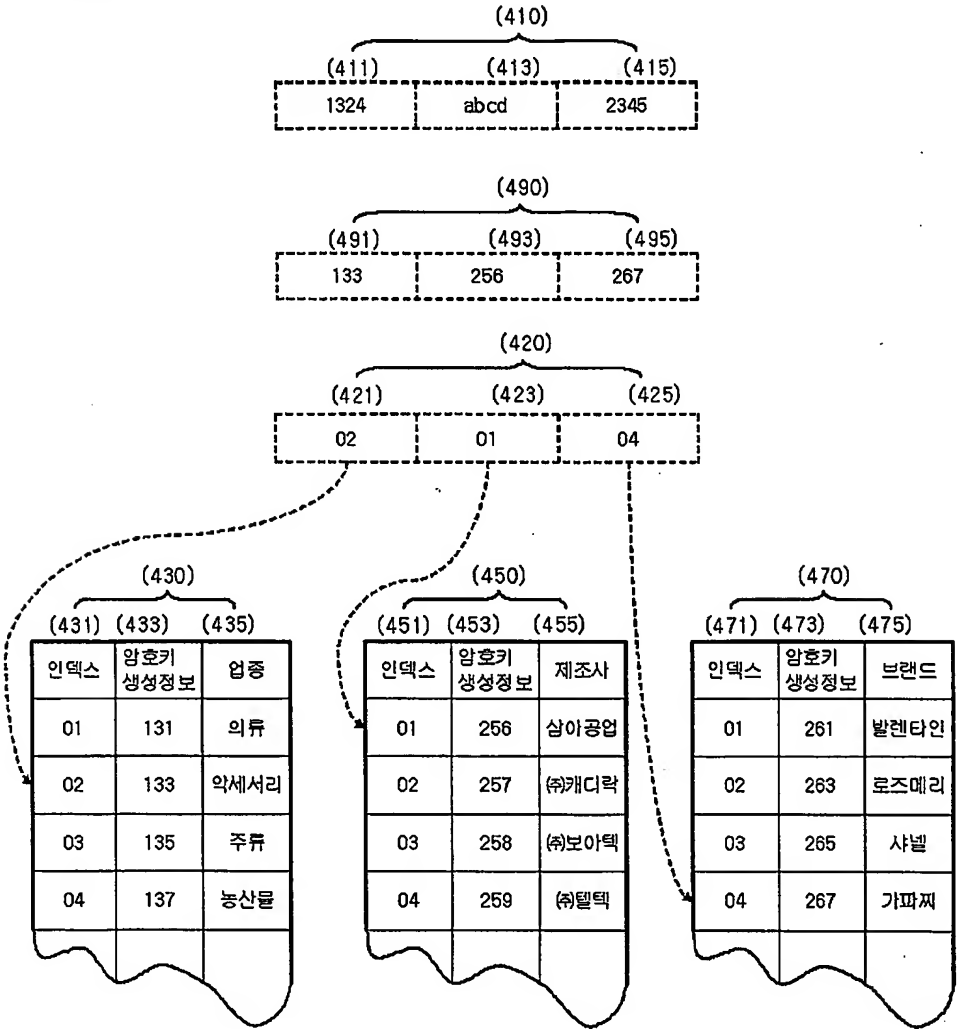
【도 5】


태그 판독기 1
태그 판독기 2
명령키 입력
S510
슬레이브 판독기 검출
S412
세션 개시
S414
암호화키의 특정요구 메시지
S432
판독기 난수 첨부
S610
암호키 특정
암호화키 특정 메시지
S434
판독기 난수 확인
태그 난수 첨부
암호키 특정
S530
체크 메시지 송신
S452
판독기 난수' 첨부
태그 난수 확인
S630
체크 메시지 복호화,
수신 표시
암호화 전송
메시지 회신
S453
복호화
난수 확인
인증 결과 표시
S550

【도 6a】


(410)
(411)
(413)
(415)
1324
abcd
2345
(420)
(421)
(423)
(425)
02
01
04
(430)
(431)
(433)
(435)
인덱스
암호키
업종
01
1234
의류
02
1324
악세서리
03
2656
주류
04
2345
농산물
(450)
(451)
(453)
(455)
인덱스
암호키
제조사
01
abcd
삼아공업
02
afce
㈜캐디락
03
ceds
㈜보아텍
04
gfds
㈜텔텍
(470)
(471)
(473)
(475)
인덱스
암호키
브랜드
01
1234
발렌타인
02
1324
로즈메리
03
2656
샤넬
04
2345
가파찌

【도 6b】


(410)
(411) (413) (415)
1324 abcd 2345
(490)
(491) (493) (495)
133 256 267
(420)
(421) (423) (425)
02 01 04
(430)
(431) (433) (435)
인덱스 암호키 생성정보 업종
01 131 의류
02 133 악세서리
03 135 주류
04 137 농산물
(450)
(451) (453) (455)
인덱스 암호키 생성정보 제조사
01 256 삼아공업
02 257 ㈜캐디락
03 258 ㈜보아텍
04 259 ㈜텔텍
(470)
(471) (473) (475)
인덱스 암호키 생성정보 브랜드
01 261 발렌타인
02 263 로즈메리
03 265 샤넬
04 267 가파찌